Studies in Systems, Decision and Control 90

Roberto Setola
Vittorio Rosato
Elias Kyriakides
Erich Rome *Editors*

Managing the Complexity of Critical Infrastructures

A Modelling and Simulation Approach

Springer Open

Studies in Systems, Decision and Control

Volume 90

Series editor

Janusz Kacprzyk, Polish Academy of Sciences, Warsaw, Poland
e-mail: kacprzyk@ibspan.waw.pl

About this Series

The series "Studies in Systems, Decision and Control" (SSDC) covers both new developments and advances, as well as the state of the art, in the various areas of broadly perceived systems, decision making and control- quickly, up to date and with a high quality. The intent is to cover the theory, applications, and perspectives on the state of the art and future developments relevant to systems, decision making, control, complex processes and related areas, as embedded in the fields of engineering, computer science, physics, economics, social and life sciences, as well as the paradigms and methodologies behind them. The series contains monographs, textbooks, lecture notes and edited volumes in systems, decision making and control spanning the areas of Cyber-Physical Systems, Autonomous Systems, Sensor Networks, Control Systems, Energy Systems, Automotive Systems, Biological Systems, Vehicular Networking and Connected Vehicles, Aerospace Systems, Automation, Manufacturing, Smart Grids, Nonlinear Systems, Power Systems, Robotics, Social Systems, Economic Systems and other. Of particular value to both the contributors and the readership are the short publication timeframe and the world-wide distribution and exposure which enable both a wide and rapid dissemination of research output.

More information about this series at http://www.springer.com/series/13304

Roberto Setola · Vittorio Rosato
Elias Kyriakides · Erich Rome
Editors

Managing the Complexity of Critical Infrastructures

A Modelling and Simulation Approach

Springer Open

Editors
Roberto Setola
Università Campus Bio-Medico
Rome
Italy

Elias Kyriakides
University of Cyprus
Nicosia
Cyprus

Vittorio Rosato
ENEA
Rome
Italy

Erich Rome
Fraunhofer-IAIS
Sankt Augustin
Germany


This book was derived from the FP7 project CIPRNet, which has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 312450. The contents of this book do not necessarily reflect the official opinion of the European Union. Responsibility for the information and views expressed herein lies entirely with the editor(s) and author(s).

ISSN 2198-4182 ISSN 2198-4190 (electronic)
Studies in Systems, Decision and Control
ISBN 978-3-319-51042-2 ISBN 978-3-319-51043-9 (eBook)
DOI 10.1007/978-3-319-51043-9

Library of Congress Control Number: 2016960289

Printed on acid-free paper

This Springer imprint is published by Springer Nature
The registered company is Springer International Publishing AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Preface

This book collects the tutorial material developed by the authors during the six editions of the Master Classes and Courses on Modelling, Simulation and Analysis of Critical Infrastructures. These training events attracted more than 200 students from all over Europe and represented the cornerstone instrument for the training program developed inside the Critical Infrastructure Preparedness and Resilience Research Network (CIPRNet) project.

CIPRNet is a Network of Excellence in the field of Critical Infrastructure Protection (CIP) composed of twelve outstanding institutions on the different topics involved in the CIP domain and co-funded by the European Union under the Seventh Framework Programme (FP7) for research, technological development and demonstration.

CIPRNet moves from the fact that our societies are increasingly dependent on the correct functioning of a huge number of technological infrastructures. Several of these infrastructures are so relevant for our wellness that they are generically indicated as a Critical Infrastructure (CI). In the last two decades for political, technological, economical and societal reasons which includes the following:

- unbundling power generation, transmission and distribution in the electrical power sector,
- globalization of the markets,
- diffusion of ICT and mobile telecommunication systems,
- introduction of "smart" paradigms (e.g. smart grids and smart cities) and
- increasing use of Internet.

We observed a significant change in these infrastructures that evolved from monopolistic and monolithic systems to open market configurations. This paradigm shift allows providing to end-user more effective, efficient, user-centric and user-friendly services with a significant reduction in costs. However, this exposes the CIs to a large number of potential dangerous threats. This happens because the actual socio-technical scenario is characterized by a large increase in (reciprocal) dependencies among the different infrastructures. This phenomenon severely contributes to increasing the complexity of the whole scenario, which, if more robust

to high-frequency low-impact events, appears more and more prone to systemic and catastrophic failure as dramatically emphasized by the pan-European and pan-America electric blackouts of 2003.

In this framework, there is also the need of increasing the capabilities of CIs to be protected against malicious enemies starting from terrorist and cyber threats. To prevent, contrast and mitigate the effect of all-hazard, CI stakeholders, CI operators and civil protection authorities need to understand the complex system of CIs and need to adapt to these changes and threats in order to be as prepared as possible to mitigate emergencies and crises affecting or emerging from CIs.

Although significant research on CI systems and on their improvement, protection and resilience has been performed in Europe in the last 15 years, the transfer of research results into practical applications lags behind expectations. One of the model examples for successful transfer of research results on Critical Infrastructure Protection into application is the facility NISAC, the National Infrastructures Simulation and Analysis Centre. It supports preparedness and protection of the nation and society by analyzing CI loss or disruption. This may also be performed in the hot phase of an emergency or crisis and enable operators to take protection, reaction, mitigation and reconstruction decisions. NISAC provides advanced capabilities based on modelling, simulation and analysis (MS&A) to CI operators, civil protection agencies and other stakeholders. It has the capacities to develop, improve and deploy these capabilities contributing to an enhanced national preparedness. Such a facility and the capabilities and capacities that NISAC provides are lacking in Europe.

CIPRNet plans to make a first step in order to change that by creating new capabilities for CI operators and emergency managers and building the required capacities for developing and deploying these capabilities. CIPRNet is linking the currently scattered European CIP research entities into an integrated virtual community with the capability of supporting national, cross-border and regional emergency management and Member States for a more effective response to large national and cross-border disaster emergencies while taking CIs into account.

Towards this end, CIPRNet integrates resources of the CIPRNet partners acquired in more than 60 EU co-funded research projects, to create new and advanced capabilities for its stakeholders with a long-lasting vision to set up a virtual centre of shared and integrated knowledge and expertise in CIP. This virtual centre shall provide durable support from research to end-users. It will be the foundation for the European Infrastructures Simulation and Analysis Centre (EISAC).

Rome, Italy — Roberto Setola
Rome, Italy — Vittorio Rosato
Nicosia, Cyprus — Elias Kyriakides
Sankt Augustin, Germany — Erich Rome
January 2017

Contents

Chapter 1
Critical Infrastructures, Protection and Resilience

Roberto Setola, Eric Luiijf and Marianthi Theocharidou

Abstract This chapter introduces the concept of Critical Infrastructure (CI). Although old civilisations had CI, the protection and resilience of CI has come to the fore again in the last two decades. The risk to society due to inadvertent and deliberate CI disruptions has largely increased due to interrelation, complexity, and dependencies of these infrastructures. The increased use of information and telecommunication technologies (ICT) to support, monitor, and control CI functionalities has contributed to this. The interest in CI and complex systems is strongly related to initiatives by several governments that from the end of the 90s of the previous century recognised the relevance of the undisturbed functioning of CI for the wellbeing of their population, economy, and so on. Their policies highlighted early the increasing complexity of CI and the challenges of providing such CI services without disruption, especially when accidental or malicious events occur. In recent years, most national policies have evolved following a direction from protection towards resilience. The need for this shift in perspective and these concepts are also analysed in this chapter.

1 Introduction

Old civilisations like the Romans already protected their Critical Infrastructure (CI) such as aqueducts and the military roads. More recently, nations planned for the protection of their key infrastructure elements such as power plants, bridges and

R. Setola (✉)
Università Campus Bio-Medico, Rome, Italy
e-mail: r.setola@unicampus.it

E. Luiijf
Netherlands Organisation for Applied Scientific Research TNO, The Hague, The Netherlands
e-mail: eric.luiijf@tno.nl

M. Theocharidou
European Commission, Joint Research Centre, Ispra, Italy
e-mail: marianthi.theocharidou@jrc.ec.europa.eu

R. Setola et al. (eds.), *Managing the Complexity of Critical Infrastructures*,
Studies in Systems, Decision and Control 90,
DOI 10.1007/978-3-319-51043-9_1

harbours in the cold war era. In the relatively quiet 80s of the previous century the protection efforts of these key points seemed to be less prominently needed. At the same time, the risk to the society due to inadvertent and deliberate CI disruptions gradually increased considerably. A number of colliding factors reinforcing the recent CI-related risk increases:

(1) the diminishing governmental control due to liberalisation and privatisation of infrastructures,
(2) the increased use of information and telecommunication technologies (ICT) to support, monitor, and control CI functionalities,
(3) the idea of the population that services can and, above all, shall be available 24/7,
(4) urbanisation which stresses the utilisation of old infrastructures to their limits,
(5) the increasing interwovenness, (supply) chaining and dependencies of infrastructural services,
(6) adversaries of the society who increasingly understand that a successful attack may create havoc.

Several of these trends and their related risk to the society were recognised by the Clinton Administration in the 90s. In response, the US Presidential Decision Directive PDD-63 [1] set forth a set of actions in 1998. The PDD-63 defined CI as "*those physical and cyber-based systems essential to the minimum operations of the economy and government*". Triggered by the PDD-63 and the millennium bug (Y2K), some other nations (e.g. Canada) started their CI studies and protection activities. In February 2001, Canada started its Office of Critical Infrastructure Protection and Emergency Preparedness (OCIPEP) within the Department of National Defence organisational structure [2]. The 11/9 event triggered more nations to put CI and their protection high on the list of their activities as the long forgotten cold war infrastructure protection plans looked outdated and ineffective [3].

While there is not a commonly accepted definition of critical infrastructure (CI), all definitions emphasise the contributing role of a CI to the society or the debilitating effect in the case of disruption [4]. On 17 November 2005, the European Commission adopted a Green Paper on a European Programme for Critical Infrastructure Protection [5]. In 2008, the European Council issued the Directive 2008/114/EC [6], which required the Member States to identify and designate European CI (ECI) and assess the needs for their protection. This Directive defined 'critical infrastructure' as:

> An asset, system or part thereof located in Member States which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions [6].

This directive referred to infrastructures of European dimension, but it triggered several Member States to identify their national CI (NCI) as well. Currently, one can find many more nations who use an equivalent of this definition without the "in a Member State" parts (see e.g. [4]). However, despite this common definition, an

open question remains: "what exactly comprises CI?". First of all, nations may define critical sectors, e.g. telecommunications, energy, transportation, drinking water, and more. Secondly, nations may define critical functions or services of these sectors (e.g. the production of isotopes for cancer treatments). Looking deeper, one may identify which components, parts, and subsystems have to be really considered as a "critical" to the critical functions of critical sectors.

Moreover, it shall be noted that the European definition not only applies to 'technical' infrastructures but also to societal and soft infrastructures.

The directive also defined the notion Critical Infrastructure Protection in an **all-hazard** perspective: "all activities aimed at ensuring the functionality, continuity and integrity of critical infrastructures in order to deter, mitigate and neutralise a threat, risk or vulnerability" [6].

2 Importance of Protection and Resilience

However, the most interesting question is why we need to increase our interest about the protection and resilience of such systems. The answer to this question can be found still in the PDD-63 that about 20 years ago stated:

> Many of the nation's critical infrastructures have historically been physically and logically separate systems that had little interdependence. As a result of advances in information technology and the necessity of improved efficiency, however, these infrastructures have become increasingly automated and interlinked. These same advances have created new vulnerabilities to equipment failure, human error, weather and other natural causes, and physical and cyber attacks" [1].

Indeed as outlined above as well as noted in [7], many economic, social, political and technological reasons have caused a rapid change in the organisational, operational and technical aspects of infrastructures. These infrastructures, that in the past could be considered as autonomous vertically integrated systems with very few points of contact with respect to other infrastructures, are now tightly coupled and show large numbers of dependencies. This has generated many positive effects to our society and the well-being of populations, but has increased the complexity, the vulnerability of infrastructures and the related risk to our societies at the same time.

Several episodes emphasised such fragility. TNO has collected more than 9,550 CI disruption events which caused the failure of 12,400 infrastructure services through cascading between 2005 and now. Some example events are described in Table 1.

Even if the example incidents illustrated in Table 1 are very different in terms of primary causes, extension and consequences, all of them are characterised by non-intuitive dependencies and, especially, by inadequate protection measures to manage the crisis. This is mainly due to the incomplete understanding of an event and especially of its direct and indirect consequences [8, 9]. This is, unfortunately, an effect of the increased complexity of the socio-technical scenario largely characterised by the presence of dependencies among different CI.

Table 1 Some example incidents of CI disruptions

1998
On May 19, 1998, the telecommunication satellite Galaxy IV spun out of control. That produced many unexpected problems in North America for several days before another replacement satellite could take over the services: about 40 million of pagers out-of-services causing major problems to dispatch doctors and nurses in hospitals and to notify first responders fast. CBS, ABC, CNN and other media networks lost nation-wide transmission signals. Air transportation was affected due to absence of high-altitude weather reports; 30 flights from Huston airport were cancelled or delayed. At the highway: drivers could not perform refuel because gas-stations lost the capability to process credit cards.
2001
On July 18, 2001, train wagons containing chloride acid derailed in a downtown tunnel in Baltimore. Fire fighters, in the absence of information about the presence of chloride acid on the train, decided to let the train burn. Unknown was also that a high-pressure water mains, a set of glass fibres and a power transmission cable were located just up the same tunnel. Due to the fire, the water transport pipeline to downtown burst open. As a result over 70 million gallons of water flooded downtown streets and houses; the drinking water supply failed, and the fire fighters lost their water supply. Glass fibres melted and caused a noticeable world-wide slowdown on the internet and caused local and international telephony outages. Over 1200 buildings lost power.
2001
The collapse of Twin-towers due to the "9/11 events" caused the inoperability of many infrastructures (electricity, water, gas, communication, steam distribution, metro, operations of key financial institutions) in a broad area of Manhattan. Moreover, the presence in that area of important telco-nodes induced degradation in telecommunication and on Internet also outside US. This large impact has been caused by the co-location of a multitude of vital CI inside the World Trade Centre. Indeed in those building there were the Port Authority Emergency Management centre, the Office of Emergency Management Operations Center, electrical power substations, steam and gas distribution, metro stations, further to be the headquarters of a number of financial institutions. Moreover also the emergency operations were affected by such extreme co-location For instance, the Verizon building 140 West St., contained 306,000 telephony and over 55,000 data lines from 30 operators and provided services to 34,000 customers in Lower Manhattan. A set of these lines was connected to antennas for first responders and mobile telephony at the roof of the towers and adjacent buildings. The communication capacity for the first responders was almost immediately lost due the fire and subsequent collapse of the WTC towers. Data and telephony services failed as the Verizon building became damaged by falling debris. Lines were cut and backup power was lost due to the flooding of batteries. Many of the communication back-up lines for first responders and agencies involved in disaster management were co-located with the primary circuits and failed. The remaining fixed and wireless communication for emergency response failed as police did not allow Verizon to refill the fuel tanks for their back-up power generators at two other, still operating, communication switch locations. During the recovery phase, police did not allow crews of all co-located operators to enter the closed-off area; only crews of Verizon were allowed to work on repairs. Verizon T-shirts allowed repair crews of AT&T and other telecommunication companies to enter the area and perform their work.
2004
In the area on Rome (Italy) during the night of 31st December there was a problem at the air-conditioning system of an important telecommunication node. The problem had not been adequately managed causing an increased degradation up to the complete collapse of the node. The telecommunication operator had no elements (neither information) to foresee which services

(continued)

Table 1 (continued)

would be impacted by the failure. They decided to not provide any warning while trying to solve the problem internally. Unfortunately they were unable to manage the situation. The direct consequence was the stop for some 6 h of all wired and mobile telephone communication in large area of Rome. Moreover as an indirect consequence, more than 5000 bank and 3000 postal offices nationwide were without communications. Moreover, 70% of check-in desks at Rome airport were inoperable (with delays for several flights). Finally they were close to an electric blackout because the electric distribution system operators abruptly lost the ability to supervise and manage of half of Rome's power grid.
2010
Mid April 2010, the Eyjafjallajoekull volcano on Island erupts through fast cooling ice cap (a so-called VEI 4 class eruption). As a result glass particles are blown into air and transported to Europe in several waves during a month. Depending on the jet stream, some 30 European nations from Sweden to Turkey had to close down their airspace affecting hundred thousands of passengers. Just-in-time transport by plane, e.g. of repair parts, as well as medicines and donor organs for transplantation could not take place. The financial loss for the tourist sector was 1 billion euro. The air transport industry lost 1.5–2.5 billion euro. The worldwide GDP impact was 5 billion US dollar.
2016
On January 4, 2016, a special weather condition caused a layer of five centimetre of black ice in the northern part of The Netherlands which impacted various CI for several days. High voltage lines develop a "wing profile" causing dangling of the lines with power dips as a result. Hospitals regard the risk of power outages too high and stopped all non-life threatening surgeries. Schools are closed. Road and rail transport was not possible to a large extent. Milk collection at farms was halted. Milk products cannot be produced anymore and distributed to supermarkets across a larger part of the Netherlands. Schools were closed for days. The air force cannot scramble their F16s anymore.

Indeed, as emphasised by the different studies performed on the emergency response after 9/11, during such a crisis there was not a clear understanding of the CI dependencies, and the need for CI protection. Moreover, the New York City emergency preparedness plans did not account for total neighbourhood and facility disasters. The emergency plans and back-up tapes with databases were inaccessible as they were in the NY city hall which was powerless and inaccessible as a result of the collapse of the two World Trade Center (WTC) towers. The Emergency Operations Center at WTC 7 was destroyed and had to be relocated three times during the emergency operations, something the operation plans did not prepare for. Finally emergency plans developed by CI operators and financial institutions did take into account the possibility of multiple CI failure, all of them considered a scenario where only their CI collapsed (see e.g. [10, 11]).

These events show that a more careful understanding of the set of CI, their dependencies and common cause failure risk along with their full operational conditions is needed. A first step is to revisit analysis reports of earlier disasters/emergencies to know the possible causes. Moreover, one can learn from the potential consequences and of decisions taken by crisis response organisations without of a clear understanding of the relationship between the different CI

services, CI elements, and actors (e.g. crisis management, CI operators). Such an analysis will stress the relevance to have a good knowledge of all the infrastructures and the services they provide, their element which operate (or are located) in a given area, and of their dependencies. This means that one has to have at least information about the geographical location of the most relevant components of the different infrastructures, as well as their function within the whole infrastructure, and possible single points of failure (also known as "key points"). Organisationally one needs to have points of contact within each of the actor organisations as "one shall not exchange business cards during an emergency".

There is the need to have methodologies and tools to support the analysis of such complex (critical) systems with earlier events as a starter. Indeed we have to consider several elements that may reduce the effectiveness of analysis performed exclusively on historical data. This is partly due to the increasing diffusion of ICT technologies, which changes significantly the operational modes of the different infrastructures. Another aspect is that high impact, low frequency events may occur that seldom that the analysis of recent events may overlook important CI dependency aspects. This effect may be amplified by the fact that near missies in CI disruptions are not reported and analysed outside the CI operator's organisation, if at all.

We also need to consider scenarios where several CI may be affects by a common mode failure event so as to take into account the operative condition of the different CI. Moreover, the relevance and impact of dependencies may largely be influenced by the actual operative conditions [12].

All these aspects call for the availability of sophisticated analysis and simulation tools, as illustrated in the next chapters of this book, while this chapter provides an overview of a selection of relevant initiatives that are on-going in the sector of CI protection and resilience.

3 Government Initiatives: Policies and Research

In this section we highlight a selection of international policies in order to identify their focus and priorities with respect to CI and CIP.

The governments of different nations recognise the increasing importance of CI protection and resilience. This is demonstrated by the policies they implement with respect to CI at sectorial and cross-sectorial levels. In parallel, these policies are frequently followed by funding to universities, national laboratories, and private companies involved in the modelling, simulation and analysis (MS&A) of CI dependencies (e.g. see [13]), which have further led to much innovative and diverse work [14].

Overall, several nations have put in place a policy for critical infrastructure protection (CIP) and also for critical information infrastructure protection (CIIP). In the recent years, we also observe a shift of the focus from CIP towards

infrastructure 'resilience',[1] even if the two concepts are not easily distinguished. The landscape of these national policies remains still very fragmented.

Moreover, government and international institutions recognised that to manage the complexity of the problem at hand there is the need to develop new methodologies, paradigms and tools. To this end several programs have been set up. Several scientific programs and institutions have been established in order to protect and strengthen CI [14]. These initiatives include, among others, the US National Infrastructure Simulation and Analysis Center (NISAC), the European Reference Network for Critical Infrastructure Protection (ERNCIP), the Critical Infrastructure Program for Modeling and Analysis (CIPMA) in Australia, the National Critical Infrastructure Assurance Program (NCIAP) in Canada, the Dutch Approach on Critical Infrastructure Protection in the Netherlands, the Critical Infrastructure Resilience Program in the UK, and the Critical Infrastructure Protection Implementation Plan in Germany. These initiatives provide a progress in the knowledge of the problems at hand so as on the possible solutions. It is interesting to note that up to 2008 the majority of R&D projects were related to security at component level [13]. Some projects focused on strategic national oriented aspects, and only few addressed problems induced by dependencies of infrastructures. The presence of such R&D programs gave rise to the methodological and technological instruments to manage the complexity emerging from dependencies among CI allowing to provide some operational tools to stakeholders, decision makers and policy makers.

3.1 The US Approach

As described above, the increased relevance of CI was recognised in the US in the mid 90s. In 1998, the Presidential Policy Directive No. 63 [1] on Critical Infrastructure Protection (CIP) recognised the need to address vulnerabilities of CI and the need for flexible, evolutionary approaches that span both the public and private sectors, and protect both domestic and international security. A detailed overview of how the CIP policy has developed in the US is presented in [17].

Currently, according to Presidential Policy Directive/PPD-21, "it is the policy of the United States to strengthen the security and resilience of its critical infrastructure against both physical and cyber threats" [18]. CI is defined by the USA PATRIOT Act[2] as:

[1]While there are no established European Union definitions of 'resilience' in the CI context, one can still find several non-official and more official definitions of the concept [15]. A suitable generic definition, applicable also for CI, is provided by UNISDR [16]: "The ability of a system, community or society exposed to hazards to resist, absorb, accommodate to and recover from the effects of a hazard in a timely and efficient manner, including through the preservation and restoration of its essential basic structures and functions" [16].

[2]§1016(e) of the United States Patriot Act of 2001 (42 U.S.C. §5195c(e)).

> Systems and assets, physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health and safety, or any combination of those matters.

As explained in [17], the US federal government works with states, local authorities, and the owners and operators of CI (in both the private and public sector) to identify those specific assets and systems that constitute the nation's CI. Together, these entities perform a risk management approach for these assets, in order to assess vulnerabilities to the threats facing the nation, assess risk, and identify and prioritise a set of measures that can be taken to mitigate risk. The approach is a voluntary one, with primary responsibility for action lying with the owners and operators of CI. The federal government, however, will intervene in case of inadequate protection or response.

According to Moteff's overview of the US policies [17], PPD-21 on Critical Infrastructure Security and Resilience made no major changes in policy, roles and responsibilities, or programs. PPD-21, however, did order an evaluation of the existing public-private partnership model, the identification of baseline data and system requirements for efficient information exchange, and the development of a situational awareness capability. PPD-21 also called for an update of the National Infrastructure Protection Plan (NIPP), and a new Research and Development Plan for Critical Infrastructure, to be updated every four years.

While not yet making any changes in policy, roles and responsibilities, and programs, the text of PPD-21 did reflect the *increased interest in* ***resilience*** *and* ***the all-hazard approach*** that has evolved in CI policy over the last few years. It also updated sector designations. However, highlighting the energy and communications sectors due to their importance to the operations of other infrastructures. The directive also required the updated NIPP [19] to include a focus on the reliance of other sectors on energy and communications infrastructure and ways to mitigate the associated risk. The latest policies have also focused efforts on expanding the cyber security policies and programs associated with CIP.

An example of research initiative is the US National Infrastructure Simulation and Analysis Center (NISAC), which is a modelling, simulation, and analysis program within the Department of Homeland Security (DHS) [20]. NISAC comprises an emergency support centre in the Washington, D.C. area, as well as Modelling, Simulation and Analysis units at the Sandia National Laboratories (SNL), Los Alamos National Laboratory (LANL), and the Pacific Northwest National Laboratory (PNNL). Congress mandated that NISAC serve as a "source of national expertise to address critical infrastructure protection" research and analysis. NISAC prepares and shares analyses of critical infrastructure, including their dependencies, vulnerabilities, consequences, and other complexities, under the direction of the Office of Cyber and Infrastructure Analysis (OCIA). To ensure consistency with CIP priorities, NISAC initiatives and tasking requests are coordinated through the NISAC program office. NISAC provides strategic, multidisciplinary analyses of dependencies and the consequences of infrastructure disruptions across all sixteen US CI sectors at national, regional, and local levels.

NISAC experts have developed and are employing tools to address the complexities of dependent national infrastructure, including process-based systems dynamics models, mathematical network optimisation models, physics-based models of existing infrastructure, and high-fidelity agent-based simulations of systems.

The NISAC is managed by the Department of Homeland Security (DHS) Office of Cyber and Infrastructure Analysis (OCIA) to advance understanding of emerging risk crossing the cyber-physical domain. NISAC's Fast Analysis and Simulation Team (FAST) provides practical information within severe time constraints in response to issues of immediate national importance using NISAC's long-term planning and analysis results, expertise, and a suite of models including impact models. Formerly known as Department's Homeland Infrastructure Threat and Risk Analysis Center (HITRAC), FAST allows to assist in emergency planning by assessing CI resilience before and during a major emergency, e.g. a Katrina or Sandy-like hurricane.

3.2 Initiatives in Europe

Reducing the vulnerabilities of CI and increasing their resilience is one of the major objectives of the EU. The European Programme for Critical Infrastructure Protection (EPCIP) sets the overall framework for activities aimed at improving the protection of CI in Europe—across all EU States and in all relevant sectors of economic activity [21]. The threats to which the programme aims to respond are not only confined to terrorism, but also include criminal activities, natural disasters, and other causes of CI disruptions. In short, it seeks to provide an **all-hazards cross-sectorial** approach. The EPCIP is supported by regular exchanges of information between EU Member States in the frame of the CIP Contact Points meetings.

EPCIP focuses on four main areas [21]:

- The creation of a procedure to identify and assess Europe's CI and learn how to better protect them.
- Measures to aid protection of CI including the establishment of expert groups at EU level and the creation of the Critical Infrastructure Warning Information Network (CIWIN)—an internet-based communication system for exchanging information, studies, and best practices in Europe [22].
- Funding for over 100 CIP projects between 2007 and 2013. These projects focused on a variety of issues including national and European information sharing and alerting systems, the development of ways to assess the dependencies between ICT and electricity transmission networks, and the creation of a 'good practices' manual for CIP policy makers [23].
- International cooperation with European Economic Area (EEA) and European Free Trade Area (EFTA) nations, as well as expert meetings between the EU, USA, and Canada.

A key pillar of this programme is the 2008 Directive on European Critical Infrastructures [6]. It establishes a procedure for identifying and designating European Critical Infrastructures (ECI) and a common approach for assessing the need to improve their protection. The Directive has a sectorial scope, applying only to the energy and transport sectors. The 2008 Directive also requires owners/operators of designated ECI to prepare Operator Security Plans (advanced business continuity plans) and nominate Security Liaison Officers (linking the owner/operator with the national authority responsible for CIP). Classified non-binding guidelines were also produced.

Taking into account the developments since the adoption of the 2006 EPCIP Communication [21], an updated approach to the EU CIP policy became necessary. Moreover, Article 11 of the 2008 Directive on the identification and designation of European Critical Infrastructures refers to a specific review process of the Directive. Therefore, a comprehensive review has been conducted in close cooperation with the Member States and stakeholders during 2012. In 2013, the European Commission evaluated the progress made by EPCIP and suggested the programme enter a new more practical phase for the future. This phase involves launching a pilot project analysing four European Critical Infrastructures (ECI) with regards to possible threats. These were:

- The EU's electricity transmission grid
- The EU's gas transmission network
- EUROCONTROL—the EU's Air Traffic Management
- GALILEO—the European programme for global satellite navigation.

Based on the results of this review and considering other elements of the current programme, the Commission adopted a 2013 Staff Working Document on a new approach to the EPCIP [24]. It sets out a revised and more practical implementation of activities under the three main work streams—prevention, preparedness and response. The new approach aims at building common tools and a common approach in the EU to critical infrastructure protection and resilience, taking better account of dependencies.

Compared with the US, the EU approach, though referring to national rather than EU legislation, seems to be a step forward towards regulative efforts instead of mere voluntary compliance, although both the US and the EU make emphasis on the importance of public-private partnerships.

In terms of cyber resilience, the European Commission has adopted a series of measures to raise Europe's preparedness to ward off cyber incidents. The Directive (EU) 2016/1148 of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union [25], also known as the NIS-directive, is the first piece of EU-wide legislation on cyber security. The Directive focuses on three priorities: (a) Member States preparedness by requiring them to be appropriately equipped, e.g. via a Computer Security Incident Response Team (CSIRT) and a competent national NIS authority; (b) cooperation among all the Member States, by setting up a cooperation group, in order to support and

facilitate strategic cooperation and the exchange of information among Member States; (c) a culture of security across sectors which are vital for our economy and society and moreover rely heavily on ICT, such as energy, transport, water, banking, financial market infrastructures, healthcare and digital infrastructure. Businesses in these sectors that are identified by the Member States as operators of **essential services** will have to take appropriate security measures and to notify serious incidents to the relevant national authority. Also key digital service providers (search engines, cloud computing services and online marketplaces) will have to comply with the security and notification requirements under the NIS-Directive. The European Commission is also examining how to strengthen and streamline cyber security cooperation across different sectors of the economy, including in cyber security training and education.

While there are similarities, the European Commission has not formally converged essential service operators and CI operators alike in [26]. Consequently, the EU Member States can adopt legislative solutions that allow a substantial coincidence of the two sets, or consider them as different set (with eventually some overlap).

In terms of research, the European Commission has funded over 100 diverse projects under the Prevention, Preparedness and Consequence Management of Terrorism and other Security-related Risks programme (CIPS), during the 2007–2012 period. The programme was designed to protect citizens and CI from terrorist attacks and other security incidents by fostering prevention and preparedness, namely by improving the protection of CI and addressing crisis management. The key objective is to support CIP policy priorities by providing expert knowledge and a scientific basis for a better understanding of criticalities and dependencies at all levels. A list of the EU co-funded projects can be found online [27]. Such projects integrate the more than 300 R&D projects co-funded by the EU Commission under the Security umbrella in the FP7 (i.e. the EU research funding agenda in the period 2007–2013). The programme covers all the aspects related with innovative technology for security, with a strong focus on security of CI. Amongst other projects co-funded under this framework is the Network of Excellence "Critical Infrastructure Preparedness and Resilience Research Network (CIPRNet)" project [28].

The interest for EU Commission about the security issues is witnessed by the inclusion of the topic security also in the H2020 programme (i.e. the Horizon 2020 programme is the EU research funding agenda for the period 2014–2020) and by the more than 150 R&D projects already granted. To be more effective, H2020 shifted the focus from technology driven perspective to a problem solving orientation with a strong requirements of active involving of security stakeholders, starting from CI operators, in order to develop solution able to concretely increase the resilience, the robustness and/or the preparedness of EU society.

Finally, a European Reference Network for Critical Infrastructure Protection (ERNCIP) has been created by the European Commission to "foster the emergence of innovative, qualified, efficient and competitive security solutions, through

networking of European experimental capabilities". It aims to link together existing European laboratories and facilities, in order to carry out critical infrastructure-related security experiments and test new technology, such as detection equipment.

3.3 The Australian Approach

This Australian Government recognises the importance of CI and focuses its policy on the essential services for everyday life provided by parts of CI. In its 2010 CI Resilience Strategy, we observe a shift towards resilience that enables an all hazards approach [29]. The Australian strategy takes into account the dependencies between critical infrastructures and sectors. It defines resilience in the context of CI, as:

> Coordinated planning across sectors and networks, responsive, flexible and timely recovery measures, and development of an organisational culture that has the ability to provide a minimum level of service during interruptions, emergencies and disasters, and return to full operations quickly.

Like in the USA and Europe, the Australian Government aims to build a public-private partnership approach between businesses and government and has established the Trusted Information Sharing Network (TISN) for Critical Infrastructure Resilience (CIR) as its primary mechanism. The goal is to establish a cross-sector approach and the identification of cross-sector dependencies.

This strategy identifies six strategic aspects:

- operate an effective business-government partnership with critical infrastructure owners and operators
- develop and promote an organisational resilience body of knowledge and a common understanding of organisational resilience
- assist owners and operators of CI to identify, analyse and manage cross-sectorial dependencies
- provide timely and high quality policy advice on issues relating to CI resilience
- implement the Australian Government's Cyber Security Strategy to maintain a secure, resilient and trusted electronic operating environment, including for CI owners and operators, and
- support the CI resilience programs delivered by Australian States and Territories, as agreed and as appropriate.

While some of these activities are a continuation of the previous CIP Program, a new strategic imperative, the one of organisational resilience, emerges.

The Critical Infrastructure Program for Modelling and Analysis (CIPMA) is part of the Australian Government's strategy to: (a) reduce exposure to risk, (b) recover from major disruptions and disasters, (c) learn from incidents. CIPMA uses a vast array of data and information to model and simulate the behaviour of CI systems and how they interrelate. Governments and CI owners and operators can use CIPMA's modelling and analysis toolset and approach to help prevent, prepare for,

respond to, or recover from, a natural or human-caused disruption to CI. It draws on all its partners to do so, including other owners and operators of CI, state and territory governments, and Australian Government agencies. CIPMA also supports the work of the Trusted Information Sharing Network (TISN) for CI resilience. The network is a forum for owners and operators of CI and governments to share information.

4 CI Resilience

As we observed in the previous section, the Australian strategy has followed a clear direction towards CI Resilience (CIR). The main argument is that due to the adverse and changing landscape of hazards and threats to CI, it is not possible to foresee, prevent, prepare for or mitigate all of these events, which in several cases can be unknown or emergent. Moreover:

> Protective security measures alone cannot mitigate supply chain disruption, nor ensure the rapid restoration of services. Owners and operators of critical infrastructure often have limited capacity to continue operations indefinitely if the essential goods and services they require are interrupted [29].

As highlighted in [30], both the USPPD-21 [18] and NIPP 2013 [19] recognise CIP "as an enabler of CIR" (Critical Infrastructure Resilience). While the US approach currently recognises resilience alongside protection, or perhaps even emphasises the former at the cost of the latter [19], it is noteworthy that this approach places its emphasis on public-private partnership in the spirit of voluntary measures from the private side. This approach is different than the European policies, which focus more on regulatory measures.

In [30] it is highlighted that the Staff Working Document [24] already includes several references to the concept of resilience and it indeed uses the phrase "CI protection and resilience" frequently. Usually these two concepts are presented together, but the document does not explicitly define either of the concepts nor make it clear how they differ from each other and how they are related. In one occasion, however, when discussing the four "relevant pan-European critical infrastructures" that are to be used as European pilot projects from 2013 onwards, it is mentioned that the respective work streams "seek to provide useful tools for improving protection and resilience, including through providing for strengthened risk mitigation, preparedness and response measures".

Currently, there are not many national, official definitions of the concept of CI Resilience, but as we observed, several national policy and strategy reports include it as a key component in their CIP programs, which depicts a shift of the CIP field towards Resilience.

Looking at the different definitions and approaches, one can notice commonalities and differences [15]. Alsubaie et al. [31] observes that properties such as 'ability to recover' and 'ability to adapt' were incorporated in several definitions. Most of the proposed definitions include 'the ability to withstand' or 'absorb' a

disturbance as a key attribute. Similarly, Bruneau et al. [32] assigns four properties to resilience for both physical and social systems: robustness, redundancy, resourcefulness, and rapidity.

In another review of resilience concepts used for CI, Francis and Bekera [33] observes the evolution in the resilience concept and also concludes that the definitions seem to converge "in the direction of a common definition, as these definitions share several common elements: absorptive capacity, recoverability, adaptive capacity, and retention of identity (structure and functions)". They argue that the objective of resilience is to retain predetermined dimensions of system performance and identity or structure in view of forecasted scenarios.

Three resilience capacities, i.e. absorptive, adaptive, and restorative capacities [33, 34] are at the centre of these approaches and are linked with the various stages of typical infrastructure response cycle to disruption (before, during and after the event). In Francis and Bekera [33] the following resilience capacities for infrastructures are defined:

- **Absorptive capacity** refers to the degree to which a system can absorb the impacts of system perturbations and minimise consequences with little effort. In practice, though, it is a management feature depending on configuration, controls, and operational procedures. System robustness and reliability are prototypical pre-disruption characteristics of a resilient system.
- While absorptive capacity is the ability of a system to absorb system perturbations, **adaptive capacity** is the ability of a system to adjust to undesirable situations by undergoing some changes. A system's adaptive capacity is enhanced by its ability to anticipate disruptive events, recognise unanticipated events, re-organise after occurrence of an adverse event, and general preparedness for adverse events.
- **Restorative capacity** of a resilient system is often characterised by rapidity of return to normal or improved operations and system reliability. This capacity should be assessed against a defined set of requirements derived from a desirable level of service or control.

In their approach, Alsubaie et al. [31] recognise that it is important to take into account the inherent interdependencies that exist among most of the modern CI. In this respect, proposed resilience concepts and measures need to incorporate CI dependencies, considering the cascade of a failure through multiple CIs, which offer different services to the community. This dependency of resilience between communities and infrastructure has been widely recognised in the scientific literature [35] and is also depicted in the Australian CIP Strategy [29].

As pointed out in [15], resilience encompass **several dimensions**; such as *technical*, *organisational*, *social*, and *economic* ones. In summary, the technological dimension refers primarily to the physical properties of infrastructure components, systems, networks or 'system-of-systems' and refer to the characteristics and behaviour of these in the case of a change or incident. This dimension is very prominent when referring to engineering resilience or to CIR and it is the aspect

most of the modelling, simulation and analysis tools and approaches focus on. Another aspect relevant to CIR is the organisational one, as it relates to the organisations and institutions that manage the physical components of the systems, i.e. CI operators or owners. It covers aspects such as culture, people, business continuity, risk, and disaster management at the organisational level. This more business-oriented aspect, which we have observed in the Australian national policy, serves as a way to gather all current business practices under one common goal: the operability of the infrastructure under adverse circumstances. The social dimension encompasses population and community characteristics that render social groups either more vulnerable or more adaptable to hazards and disasters. We observe that national resilience policies recently include, except of economic or even environmental aspects, social aspects in their definitions of resilience as CI are vital for maintaining key societal functions. These refer to the community and highlight how infrastructures contribute with essential services to it, e.g. as discussed in the aforementioned NIS Directive.

Overall, a resilience-based approach for CI is an approach that is gradually adopted by nations in order to face the challenges and costs of achieving maximum protection in an increasingly complex environment and to overcome limitations of the traditional scenario-based risk management approach, where the organisation may lack capabilities to face risk from unknown or unforeseen threats and vulnerabilities.

5 Conclusion

This chapter introduced the concept of Critical Infrastructure (CI) and their protection. It has illustrated which factors contribute to the complexity of modern infrastructures, as well as the needs that drive scientists to develop modelling, simulation and analysis (MS&A) tools for this area. This interest in CI and complex systems is strongly related to initiatives, by several governments that from the end of the 90s of the previous century recognised the relevance of the undisturbed functioning of CI for the wellbeing of their population. They also stimulated the research community and gave rise to several projects, a selection of which was presented in this chapter.

In the past years, international policies and their respective research programs have shifted towards a resilience-based approach. While the different nations continue to work in areas such as risk management, protection, dependency modelling and analysis, etc., resilience gains a more prominent role, as the ‘umbrella’ term to cover all the various aspects and the various stages of crisis management when a critical infrastructure faces a disruptive event.

In the following chapters, we will focus on modelling, simulation and analysis and explore how such methods and tools can contribute to a better understanding of CI complexity and can be used in order to improve the protection and resilience of infrastructures.

Acknowledgement and Disclaimer This chapter was derived from the FP7 project CIPRNet, which has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no. 312450.

The contents of this chapter do not necessarily reflect the official opinion of the European Union. Responsibility for the information and views expressed herein lies entirely with the author (s).

References

1. White House (1998) The Clinton's Administration's Policy on critical infrastructure protection: presidential decision directive 63/PDD-63, White paper, 22 May 1998. Available online at http://fas.org/irp/offdocs/pdd/pdd-63.htm. Retrieved on 27 Oct 2016
2. Rossignol M (2001) Critical infrastructure and emergency preparedness, report PRB 01-7E, Canada, June 2001. Available online at http://publications.gc.ca/Collection-R/LoPBdP/EB/prb017-e.htm. Retrieved on 27 Oct 2016
3. Brunner EM, Suter M (2008) International CIIP handbook 2008/2009. Center for Security Studies, ETH Zurich. Available online at http://www.css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/CIIP-HB-08-09.pdf. Retrieved on 27 Oct 2016
4. CIPedia©, 2016. Available online at www.cipedia.eu. Retrieved on 27 Oct 2016
5. European Commission (2005) COM 576 final, Green paper on a European Programme for critical infrastructure protection, Brussels, 17.11.2005. Available online at http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52005DC0576&from=EN. Retrieved on 27 Oct 2016
6. European Council (2008) Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection (Text with EEA relevance), Brussels, Dec 2008. Available online at http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32008L0114&from=EN. Retrieved on 27 Oct 2016
7. Bologna S, Setola R (2005) The need to improve local self-awareness in CIP/CIIP. First IEEE international workshop on critical infrastructure protection (IWCIP'05). IEEE
8. Luiijf HAM, Nieuwenhuijs AH, Klaver MHA, van Eeten MJG, Cruz E (2010) Empirical findings on European critical infrastructure dependencies. Int J Syst Syst Eng 2(1):3–18
9. Van Eeten M, Nieuwenhuijs A, Luiijf E, Klaver M, Cruz E (2011) The state and the threat of cascading failure across critical infrastructures: the implications of empirical evidence from media incident reports. Public Adm 89(2):381–400
10. US General Accounting Office (2003) Potential Terrorist Attacks: Additional Actions Needed to Better Prepare Critical Financial Market Participants, report GAO-03-251, Washington DC, Feb 2003. Available online at http://www.gao.gov/new.items/d03251.pdf. Retrieved on 27 Oct 2016
11. OCIPEP (2002) The September 11, 2001 Terrorist attacks—critical infrastructure protection lessons learned, IA02-001, 27 Sept 2002, Ottawa. Available online at http://www.au.af.mil/au/awc/awcgate/9-11/ia02-001_canada.pdf. Retrieved on 27 Oct 2016
12. Nieuwenhuijs AH, Luiijf HAM, Klaver MHA (2008) Modeling critical infrastructure dependencies. In: Mauricio P, Shenoi S (eds) IFIP international federation for information processing. Critical infrastructure protection II, vol 290. Springer, Boston, pp 205–214
13. Setola, R, Luiijf E, Bologna S (2008) R&D activities in Europe on critical information infrastructure protection (CIIP). Int J Syst Syst Eng Nos. 1/2:257–270
14. Ouyang M (2014) Review on modeling and simulation of interdependent critical infrastructure systems. Reliab Eng Syst Saf 121:43–60

15. Theocharidou M, Melkunaite L, Eriksson K, Winberg D, Honfi D, Lange D, Guay F (2015) IMPROVER deliverable D1.2 first draft of a lexicon of definitions related to Critical Infrastructure Resilience, 30 Nov 2015
16. UNISDR Terminology on Disaster Risk Reduction, United Nations International Strategy for Disaster Reduction (UNISDR), Geneva, Switzerland, May 2009. Available online at http://www.unisdr.org/we/inform/publications/7817. Retrieved on 27 Oct 2016
17. Moteff JD (2015) Critical infrastructures: background, policy, and implementation, congressional research service, 7-5700, RL30153, 2015. Available online at https://www.fas.org/sgp/crs/homesec/RL30153.pdf. Retrieved on 27 Oct 2016
18. White House (2013) Presidential policy directive/PPD-21, critical infrastructure security and resilience, 12 Feb 2013. Available online at https://www.dhs.gov/sites/default/files/publications/ISC-PPD-21-Implementation-White-Paper-2015-508.pdf. Retrieved on 27 Oct 2016
19. Department of Homeland Security, NIPP 2013: partnering for critical infrastructure security and resilience, 2013. Available online at https://www.dhs.gov/sites/default/files/publications/National-Infrastructure-Protection-Plan-2013-508.pdf. Retrieved on 27 Oct 2016
20. Web page. Available online at http://www.sandia.gov/nisac/. Retrieved on 27 Oct 2016
21. European Commission, Communication from the Commission of 12 December 2006 on a European Programme for Critical Infrastructure Protection, COM (2006) 786 final—Official Journal C 126 of 7.6.2007. Available online at http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52006DC0786&from=EN. Retrieved on 27 Oct 2016
22. Web page. Available online at http://ec.europa.eu/dgs/home-affairs/what-we-do/networks/critical_infrastructure_warning_information_network/index_en.htm. Retrieved on 27 Oct 2016
23. Klaver M, Luiijf E, Nieuwenhuijs A (2016) Good practices manual for CIP policies for policy makers in Europe, TNO, 2011. Available online at http://www.tno.nl/recipereport. Retrieved 27 Oct 2016
24. European Commission, Staff Working Document on a new approach to the European Programme for Critical Infrastructure Protection Making European Critical Infrastructures more secure, Brussels, 28.8.2013, SWD (2013) 318 final. Available online at http://ec.europa.eu/transparency/regdoc/rep/10102/2013/EN/10102-2013-318-EN-F1-1.PDF. Retrieved on 27 Oct 2016
25. Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union ["NIS Directive"], Brussels, July 2016. Available online at http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&from=EN. Retrieved on 27 Oct 2016
26. Luiijf E, van Schie T, van Ruijven T, Huistra, A (2016) The GFCE-MERIDIAN good practice guide on critical information infrastructure protection for governmental policy-makers. TNO. Available online at https://www.tno.nl/gpciip. Retrieved on 27 Oct 2016
27. European Commission, Examples of CIPS projects. Available online at http://ec.europa.eu/dgs/home-affairs/financing/fundings/projects/per-program/cips/index_en.htm#/c_. Retrieved on 27 Oct 2016
28. Critical Infrastructure Preparedness and Resilience Research Network (CIPRNet) website, 2016. Available online at www.ciprnet.eu. Retrieved on 27 Oct 2016
29. Australian Government (2010) Critical infrastructure resilience strategy. ISBN: 978-1-921725-25-8. Available online at: http://www.emergency.qld.gov.au/publications/pdf/Critical_Infrastructure_Resilience_Strategy.pdf. Retrieved on 27 Oct 2016
30. Pursiainen C, Gattinesi P (2014) Towards testing critical infrastructure resilience, EUR—Scientific and Technical Research reports, European Commission, Joint Research Center
31. Alsubaie A, Alutaibi K, Marti J (2016) Resilience assessment of interdependent critical infrastructure. In: Rome E, Theocharidou M, Wolthusen S (eds) Critical information infrastructures security, 10th international conference, CRITIS 2015, Berlin, Germany, 5–7 Oct 2015, Revised Selected Papers, pp 43–55

32. Bruneau M, Chang SE, Eguchi RT, Lee GC, O'Rourke TD, Reinhorn AM, Shinozuka M, Tierney AM, Wallace AM, Von Winterfeldt D (2003) A framework to quantitatively assess and enhance the seismic resilience of communities. Earthq Spectra 19(4):733–752. Available online at http://doi.org/10.1193/1.1623497. Retrieved on 27 Oct 2016
33. Francis R, Bekera B (2014) A metric and frameworks for resilience analysis of engineered and infrastructure systems. Reliab Eng Syst Saf 121:90–103. Available online at http://dx.doi.org/10.1016/j.ress.2013.07.004.367. Retrieved on 27 Oct 2016
34. Ouyang M, Dueñas–Osorio L, Min X (2012) A three–stage resilience analysis framework for urban infrastructure systems. Struct Saf 36–37, 23–31 May–July. Available online at http://dx.doi.org/10.1016/j.strusafe.2011.12.004. Retrieved on 27 Oct 2016
35. Melkunaite L (ed) (2016) IMPROVER deliverable D1.1 international survey, 31 May 2016. Available online at http://media.improverproject.eu/2016/06/IMPROVER-D1.1-International-Survey_DRAFT.pdf. Retrieved on 27 Oct 2016

Chapter 2
Modelling Dependencies Between Critical Infrastructures

Roberto Setola and Marianthi Theocharidou

Abstract This chapter provides an overview about dependencies among infrastructures and discusses how they can be adequately captured, modelled and analyzed. It provides a taxonomy overview of the most adopted methods with a focus on the IIM (Input-output Inoperability Model) and on topological approaches.

1 Introduction

Dependencies among infrastructures are usually complex and non-obvious. They may allow cascading disruptions or failures to different infrastructures, thus causing a potentially significant impact to multiple types of sectors, individuals or countries. Well-known examples of such cascading effects include the electric power disruptions in California in 2001 [1], as well as the major blackouts in the USA, Canada and Europe in 2003 [2].

Identifying CI dependencies leads to a more accurate assessment on the criticality level of a single infrastructure element, or even of a whole sector. It also enables the identification of dependency chains among dependent CIs. In this way it becomes possible to identify the 'most' critical among the infrastructures and adopt more cost-efficient security controls, so as to reduce overall risk [3]. The identification of such dependencies is also important during the risk assessment and planning phase so as to ensure that the mitigation and the recovery processes take into account such relationships among infrastructures. Recently, dependency models are increasingly

R. Setola (✉)
University Campus Bio-medico of Rome, via A. del Portillo 21,
00128 Rome, Italy
e-mail: r.setola@unicampus.it

M. Theocharidou
European Commission, Joint Research Centre, via E. Fermi, 2749,
21027 Ispra, VA, Italy
e-mail: marianthi.theocharidou@jrc.ec.europa.eu

R. Setola et al. (eds.), *Managing the Complexity of Critical Infrastructures*,
Studies in Systems, Decision and Control 90,
DOI 10.1007/978-3-319-51043-9_2

used to support emergency managers in order to better prepare and plan for possible cascading effects [4].

This chapter provides an overview about the types of dependencies that can be observed among infrastructures. It also analyses the different approaches which are currently applied for modeling, with a focus on the IIM (Input-output Inoperability Model) and on network based approaches. These approaches were selected because of their comprehensiveness; indeed due to their simplicity they can be a starting point when studying modeling for Cls (see also Chap. 6 for more information on the topic).

2 Why Are Dependencies Important?

The well-known electric failure scenario of California [1] is an illustrative, real case of complex and multi-order dependency. The electric power disruptions in California caused cross-sectoral cascading consequences, affecting the natural gas production, the operation of petroleum product pipelines transporting gasoline and jet fuel within California, Nevada and Arizona, and the operation of massive pumps used to move water to crop irrigation (*first-order dependencies*). Gas production curtailed by power losses directly impacted gas supplies for generating units, further exacerbating power problems (*feedback loop*). Tight natural gas supplies also had the capability to shut down gas-fired industrial co-generation units producing steam to be injected into California's heavy oil fields (*second-order dependencies*), thus potentially reducing heavy oil recovery (*third-order dependencies*). Similarly, the disruption of pipelines caused inventories to build up at refineries and draw down at the product terminals (*second-order dependencies*), including several major Californian airports. Declining jet fuel stocks at airports entailed several major airline operators to consider contingency plans in the case of fuel shortages (*third-order dependencies*).

In the same way, the blackouts in the USA-Canada (August 2003), Southern Sweden and Eastern Denmark (September 2003) and Italy (September 2003) highlight the possibility of international cascading effects. These examples depict how a single event or incident occurred in one infrastructure, whose effect may have been assessed to cover a (geographically or sectoral) limited number of entities, is in fact affecting many other CIs. In all three blackouts, we observe a chain of failures causing cross-border effects and a significant impact to people.

The impact of a disruption, or failure, may spread both geographically and across multiple sectors. Identifying dependencies is therefore an important task. However, in many cases special types of dependencies are not obvious and easy to identify. For example, socially derived or human-initiated dependencies may refer to changes in behavior of individuals, which can be observed during a crisis. Such changes in behavior may consequently affect infrastructures or networks in a different way than the one initially perceived. A disruption in the transportation sector may cascade to wireless communication networks [5], due to alterations on calling

patterns and activities, which may affect the load on wireless networks and cause disruptions in communication.

Although the identification of first-order interdependencies may be sufficient, in order to assess the risk of a particular CI, they may fail to capture cascading effects at a macroscopic level. For example, one or more, relatively minor, incidents on one CI may cause cascading and escalating impacts to a dependent CI of a second or third level. Even worse, a second or third-level effect may in turn affect the initiating source of the problem and in this way cause a feedback effect, which will further increase the total impact of the incident.

The identification is even more complex due to the fact that dependencies may also shift on the mode of operation of the CI [6]. An example of this shift in dependency, is that in case of power loss, a hospital is dependent on diesel fuel when running on emergency power.

3 Dependencies and Interdependencies

In the literature several definitions of "dependency" and "interdependency" were presents; however one of the most widely accepted is [7]:

Dependency is the capability of an infrastructure to influence the state of other infrastructures. Then infrastructure A depends on infrastructure B when a variation in this latter has the capability to influence (e.g. modify) some states (e.g., behaviours, characteristics, properties, etc.) of infrastructure A. It is, therefore, a unidirectional relationship.

Dependencies between two infrastructures (or their functions/services) may be direct or indirect (see Fig. 1). Infrastructure C may be directly dependent on infrastructure A (**direct dependency**), or dependent of infrastructure B (or a recursively a chain of infrastructures) which in turn is dependent on infrastructure A (**indirect dependency** C of A). Notice that in this last case we indicate that B has a second order dependency on A, i.e. the number of "hop" in the dependency chain represent the order of dependency.

On the other side the term **interdependency** represents a bidirectional relationship between two or more infrastructures where the state of each infrastructure is influenced or is correlated to the state of the other. Hence, infrastructures A and B are interdependent if A depends on B and, at the same time, B depends on A, As shown in Fig. 1, such bi-directional dependency can be mediated by other infrastructures.

Notice that the presence of interdependency creates loops of reciprocal influence. In the presence of loops the consequence of any fault it can no longer be described via described via a tree structure (where there is a root and the consequences go only downstairs) although the propagation has a graph structure, i.e. the consequences have no preferential direction. This implies that negative consequences in any infrastructure are exacerbated.

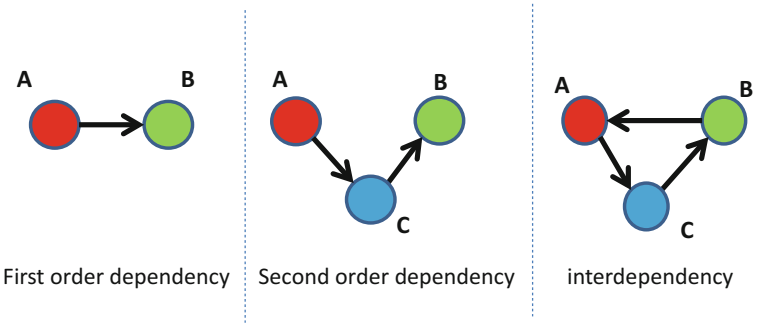


Fig. 1 Dependency and interdependency

In the framework of Critical Infrastructure Protection (CIP), we generally limit our attention only on the phenomena strictly related to services and functionalities degradation. In other terms, we consider a steady-state configuration for the overall system and we characterise dependencies and interdependencies on the basis of the effect that a failure (accidental event or malicious attack) in a component/infrastructure induces on the other elements in terms of worsening degradation of their functionalities.

Going further into detail in [1] it is emphasised that interdependencies should be analysed with respect to six different dimensions, which include characteristics of the infrastructures, of the environment, the type of failure, the operative condition and the phenomena that generate the coupling. In particular, they catalogue such phenomena into four not mutually exclusive classes:

- *Physical interdependency*—Two infrastructures are physically interdependent if the operations of one infrastructure depend on the physical output(s) of the other.
- *Cyber (inter)dependency*—An infrastructure presents a cyber-interdependency if its state depends on information transmitted through the information infrastructure.
- *Geographical (inter)dependency*—A geographical interdependency occurs when elements of multiple infrastructures are in close spatial proximity. In this case, particular events, such as an explosion or a fire in an element of an infrastructure, may create failures in one or more infrastructures in close proximity.
- *Logical (inter)dependency*—Two infrastructures are logically interdependent if the state of each one depends on the state of the other via control, regulatory or other mechanisms that cannot be considered physical, geographical or cyber.

In addition in [8] an additional category of dependencies is introduced:

- *Social dependency.* The link between the CIs is based on impacts caused by human behaviour. For example, the state of a CI is affected by the spreading of disorder to another CI related to human activities. This models the (irrational)

human behaviors in the case of crisis, e.g. overloading communication system or collective panic reactions.

In [1] it is stressed that cyber interdependency tends to become an absolute and global characteristic of all the infrastructures, while other types of interdependencies are more local. Cyber dependency potentially couples an infrastructure with every other infrastructure that uses the cyberspace, in spite of their nature, type or geographical location.

A different, but similar, classification can be found in [9] where the authors consider: Physical, Geospatial, Policy, and Informational.

Using a dataset on CI disruption incidents, empirical analysis [10, 11] showed that interdependencies—mutual dependencies—seldomly occur. Newer analysis shows that the only interdependencies that are mentioned in press reports occur at a lower, component or subsystem, level of abstraction. No 'shooting in one's own foot' has been observed where A depends on B, B on A, and the disruption of A causes B to get disrupted causing A not being able to recover at all as B's critical functions are disrupted.

Using this understanding, Nieuwenhuijs et al. [6] concluded that the set of 'interdependencies' presented by Rinaldi et al. on 2001 needed a reassessment. They stated that the geographical interdependencies are not dependencies but they are the result of a **common mode failure** (e.g. astorm) and that the mentioned 'interdependencies' are just 'dependencies'. Dependencies are not a binary on/off phenomenon but shall be seen as the service level of quality (or set of qualities), e.g. the triple pressure, biological purity, and chemical purity of drinking water. Only when the service level drops below the expected service level, a dependency may cause a 'cascading' disruption in the dependent function, service, or infrastructure. The degradation and recovery characteristics for each quality are infrastructure specific functions, such as the slow loss of pressure in drinking water pipelines after the failure of the distribution grid pumps amplified by on-going demand, and the slow system recovery as repressuring takes time. Their analysis also shows that those who analyze CI dependencies also need to take into account the **mode of operation**. The daily set of dependencies (normal operations) may be very different from the set of dependencies when a CI has been disrupted (stress mode of operation), the dependencies in the crisis mode of operation, and during the recovery. For instance, a hospital is not dependent on diesel fuel, diesel trucks, truck drivers and lumbermen for their normal operations. But when a big storm hits and downs power lines, the backup generator starts. When the diesel tank starts to run dry, the hospital needs to order diesel, requires diesel transport (fuel loading, truck, driver) and a road cleared from toppled trees. Alike, for recovery, one may need an extraordinary large crane to repair critical infrastructure. To identify such sets of shifting dependencies it is required the analysis of the scenarios beyond the analysis of a disruption of a single CI.

In [12], it is emphasised that, to correctly understand the behaviour of these infrastructures, it is mandatory to adopt a three-layer model:

- *Physical layer*—the physical component of the infrastructure, e.g., the grid for the electrical network.
- *Cyber layer*—hardware and software components of the system devoted to control and to manage the infrastructure, e.g., SCADA and DCS.
- *Organisational layer*—procedures and functions used to define activities of human operators and to support cooperation among infrastructures.

Here, the authors emphasise that each component of an infrastructure interacts, further than the other components of its infrastructure in the same layer also with the components of its infrastructure posed in the other layers (by means of internal links indicated as "inter-dependency"). Moreover, any component also interact with elements in the same physical/cyber/organizational layers of other infrastructures, by means of external links denoted as "extra-dependency". The increasing presence of these latter links creates many functional dependencies among infrastructures. Moreover, the authors emphasise that, with respect to ten years ago, the importance of the cyber layer is largely increased, becoming one of the most important sources of interdependencies. Notice that a similar kind of decomposition was also used to analyse the 2003 blackout in the USA and in Canada [13]. As a matter of fact, to explain the multitude of causes that produced that episode, the joint of USA and Canada governmental investigative commission described the event in terms of grid (physical), computer and human layers. Only by considering all the layers together it is possible to correctly understand what really led to the blackout.

The dependence-related disruptions or outages have also been classified as *cascading*, *escalating* or *common-cause* [1]:

- A cascading failure is defined as a failure in which a disruption in an infrastructure A affects one or more components in another infrastructure, say B, which in turn leads to the partial or total unavailability of B.
- An escalating failure is defined as a failure in which an existing disruption in one infrastructure exacerbates an independent disruption of another infrastructure, usually in the form of increasing the severity or the time for recovery or restoration of the second failure.
- A common-cause failure occurs when two or more infrastructure networks are disrupted at the same time: components within each network fail because of some common cause. This occurs when two infrastructures are co-located (geographic interdependency) or because the root cause of the failure is widespread (e.g., a natural or a man-made disaster).

A more recent empirical study [11], shows that events can been classified as *cascade initiating* (i.e., an event that causes an event in another CI), cascade resulting (i.e., an event that results from an event in another CI), and independent (i.e., an event that is neither a cascade initiating nor a cascade resulting event). The empirical findings indicate that:

1. cascade resulting events are more frequent than generally believed, and that cascade initiators are about half as frequent.
2. the dependencies are more focused and directional than often thought.
3. energy and telecommunication are the main cascading initiating sectors.

Luiijf et al. [14] also argue that most current dependency models neglect to recognize multiple states of operation. They usually focus on identifying dependencies under normal operational conditions, failing to model the dependencies that may emerge as soon as the operation of an infrastructure deviates from these conditions. They highlight that cascading failures may occur due to CI operators not realizing that they face different sets of dependencies in each operational state. To this end, they identify four different states of CI operation to be considered when performing dependency modeling:

- *Normal*: the state in which a CI operates under normal operational conditions.
- *Stressed*: state in which a CI operates when special measures have to be taken to keep the operation under control.
- *Crisis*: this is the state where the operation is out of control.
- *Recovery*: this is the state where the operation is again brought under control but has not yet been restored to the normal state.

A related work in identifying and modeling dependencies includes the use of sector-specific methods, e.g., gas lines, electric grid or ICT, or more general methods that are applicable in various types of CIs. In the following section, we review and illustrate some of the most popular methods to model dependencies phenomena.

4 Dependency Modeling Approaches

As noted in [1] the relevance, mechanism and effect of the dependency varies according to geographical scope under analysis. Generally more large is the area of reference, more relevant are the phenomena induced by the presence of (inter) dependencies.

Different approaches have been used to examine dependencies under a microscopic or macroscopic point of view. De Porcellinis et al. [8] refer to reductionistic and holistic approaches. A reductionistic approach identifies elementary components within a CI and then describes the evolution of the entire system based on the aggregated behaviour of these components. Holistic examples include the study dependencies between different CIs [6], within the same or different sectors of a country [15]. Many holistic approaches apply Leontief's inoperability input-output model (IIM), which calculates economic loss due to unavailability on different CI sectors based on their interdependencies.

In the literature, a uniform data collection method has not been implemented, which means that a significant effort needs to be placed to sort, evaluate or combine

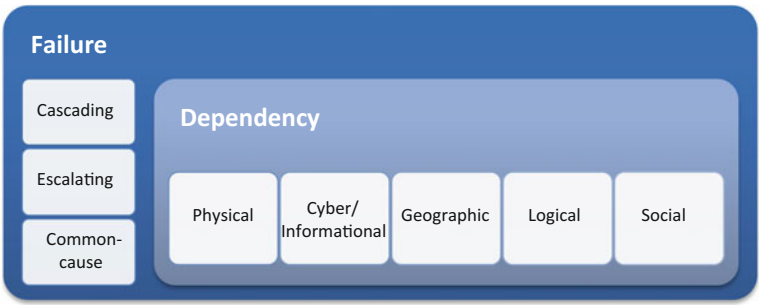


Fig. 2 Taxonomy of dependency and failure adapted by [1, 8]

these data. Since most of these approaches are historically based they can be used in order to predict similar, known failures, but they do not provide good prediction capability for unknown or new incidents. These weaknesses call for other simulation approaches for additional decision support, which we will also examine later in this chapter (Fig. 2).

On the base of the approaches used to investigate the dependency phenomena we can identify three main categories of modeling: Holistic, Topologic and Simulation-based.

Holistic approaches These approaches adopt more simplified models able to provide, with some approximation, qualitative information about the phenomena. Generally, they assume that each infrastructure can be modeled as a single entity, which depends for its correct behavior or performance on the availability of services provided by other infrastructures (other entities).

They generally adopt economic or empirical data as source of information to infer dependencies, such as history data of failures, incidents or disruptions, as well as experts opinions. A typical example of such approaches is the economic and 'inoperability' metrics used for dependency modeling [16]. Ouyang [17] argues that such empirical studies are used in order to: "identify frequent and significant failure patterns, quantify interdependency strength metrics to inform decision making, make empirically-based risk analysis, and provide alternatives to minimize the risk".

Holistic approaches generally operate with macro-scale aggregated information that can be acquired with relatively reduced effort [18]. This largely facilitates the set-up of the models. They are usually the starting point of such analysis and they can be used when sensitive data cannot be exchanged among stakeholder because of the possibility of agreeing an acceptable level of abstractions. At the same time, it may be introduced a bias to the results, over- or under-estimating some aspects with respect to others. The information obtained by such methodologies is not suitable for operative analysis.

Network-based approaches These approaches assume that each infrastructure is composed by a set of identical elements (generally represented as a node on a

graph), while dependencies are inferred assuming some sort of relationship existing among nodes belonging to different networks [19, 20, 21]. **Topology-based or structural** approaches generally identify discrete states for each component (node or link) and usually with two states: failed and normal, i.e., each node is either fully working or completely out-of-work. To implement these approaches in their basic formulation it is enough to have the topological structure of the infrastructure (which is a quite easy data to obtain). This static formulation is able to capture the 'structural' properties of the network. These approaches usually examine failures at the node or link level, and then examine cascading failures to other nodes or links within the network. They are used to evaluate the robustness of a network from the topological perspective, e.g. using centrality measures [22]. Further useful methods are illustrated in Chap. 6.

However, in several cases, e.g., for a telecommunication network, topologic analyses are unsatisfactory because the static properties of the network do not have immediate consequences on its capability to provide the intended services. To overcome such limit, some authors as Rosato et al. [23] suggested to consider also network dynamics and, to this end, they equipped the topological structure with some kind of flow dynamic models (**flow-based** models) (see also [17]). Flow-based methods depict the level of services exchanged between nodes or the flow in the graph. In this case, each node can deliver to, or consume a service from another node. Such approaches offer a depiction, which is closer to reality, and they are also used to identify critical nodes or links in the graph. The problem is that the data required to tune such dynamic models is hard to obtain and the computational cost is very high as the network grows. In most cases, and depending on the level of detail, such network-based approaches are analyzed further by simulation methods.

Simulation-based approaches These approaches try to discover the dependency phenomena as emerging from the behavior of single components and parts. Hence, they are generally able to consider a continuous level of degradation in the component functionalities and the concurrent presence of several types of phenomena (like absence of resources, external failures and internal dynamics). Starting from the component-based behavior, they try to obtain information about the 'dependence' existing among the infrastructures. Generally, these approaches are intrinsically quantitative and operation oriented. Substantially these methodologies use simulation framework to estimate the impact induced by a given failure to a scenario composed by several heterogeneous infrastructures (see [24–27]). Unfortunately, for the phenomena under analysis, a more detailed model does not necessarily mean a more accurate model. Indeed, the complexity of such simulation platforms mask, in several cases, a large number of subjective hypotheses, which influences the correctness of the solutions.

As illustrated in Fig. 3, holistic approaches are more easy to develop and set-up due their level of abstraction, but they are fundamentally strategy-oriented. On the other side, simulation-based solutions are able to give operative information, but they require more computational overhead and more detailed models. The latter represents a serious drawback because, in the field of critical infrastructure, it is

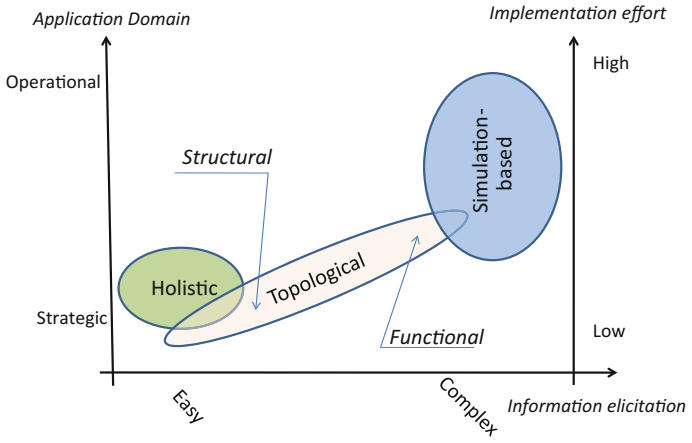


Fig. 3 Taxonomy of dependency modeling approaches [7]

very difficult to collect such detailed data due to the reluctance of the operators to provide such sensitive data, and also because of the huge quantity of highly time-varying data that should be collected. In the middle, we have the networked based approaches, which, for some aspects, share some of the advantages and weaknesses of both previous classes. Indeed, their most simple formulation (that referred as 'structural') is quite easy to set-up, since only the topological structure of the involved systems is required. Conversely, when there is the need to consider also the 'functional' properties of the network, the complexity of the model grows fast and it becomes comparable with simulation-based approaches. The topological approach, in a scenario composed of two infrastructures, where there is a single predominant (e.g., physical) dependency mechanism, is able to provide more 'objective' measurements rather than holistic models of comparable effort. Unfortunately, the extension to more complex scenarios is not straightforward and requires to collected huge quantity of resources.

In the rest of the chapter we illustrate in more detail the first two classes (which will be further analyzed in Chap. 6), while the other chapters of the book are dedicated to illustrate the different elements and aspects related with the simulation based approach.

In [17] the authors have catalogued about 150 approaches using a six classes taxonomy where the methods are not split on the level of granularity of the data but on the type of information used in the six classes:

- *Empirical approaches*: The analysis of the dependencies is performed on the base of historical accidents or disaster data and past expert experiences. These methods allow to identify frequent and significant failure patterns, to quantify (inter)dependency indicators and perform empirically-based risk analyses;
- *Agent based approaches*: These approaches follow a bottom-up method assuming that the complex behavior emerges from many individual and

relatively simple interactions of autonomous agents (i.e. adopting a complex adaptive systems (CAS) methodology).
- *System dynamics approaches*: which use System Dynamic framework to analyze complex systems involving interdependencies on the base of top-down method.
- *Economic theory based approaches*: where dependencies are identified on the base of economic exchanges among sectors and infrastructures on the base of Input–output methods.
- *Network based approaches*: Infrastructure are described by networks, where nodes represent different components and show the existing (physical) relationship among them. Such class includes topology-based and flow-based methods.
- Other approaches: which collect other methods based on hierarchical holographic modeling (HHM), high level architecture (HLA), petri-net (PN), dynamic control system theory (DCST), Bayesian network (BN), etc. For more details see [17] and the reference therein.

Other classifications of approaches are also available in the literature [52–54].

5 Holistic Approaches

Holistic approaches are based on the concept of 'service degradation', in order to illustrate how degradation within one infrastructure (or sector or component) is able to influence the capability to operate of other infrastructures.

These approaches are generally abstract, simplified and strategic oriented. They can be set-up quite easily, as they do not require as detailed data as other approaches. Even if several important aspects are neglected (e.g., the geographical dispersion that characterizes several infrastructures), they are "compact and understandable"; moreover, they can consider, at the same time, several infrastructures and dependency mechanisms (even if they all reduce to a single abstract parameter, e.g., inoperability). Finally, these approaches are service oriented.

IIM In this framework, the most popular approach is the input-output inoperability model (IIM), introduced in [16] as an evolution of the economic theories of the Nobel Prize Leontief [28]. IIM uses the same theoretical framework proposed by Leontief, but instead of considering how production of goods of a firm influences the level of production of the other firms, it focuses on the spread of operability degradation among the networked system. The most significant idea introduced in this paper was the concept of 'inoperability', intended as the inability of an element to perform its prescribed functions. This concept can be assumed as one of the 'lowest common denominator' allowing to measure with a single abstract parameter several types of relationships. For the same intent in Macaulay [18], the author suggests to use a monetary equivalent.

With a high level of approximation, the approach assumes that each infrastructure is modeled as a single entity, whose level of operability depends on the

availability of "resources" supplied by the other infrastructures. Then, an event (e.g., a failure) that reduces the operational capability of the i-th infrastructure may induce degradation also in the other infrastructures, which require goods or services produced by the i-th one. These degradations may be further propagated to other infrastructures (cascading effect) and even exacerbate the situation of the i-th one due to the presence of feedback loops.

Mathematically, IIM describes these phenomena on the basis of the level of inoperability associated to each infrastructure. Following the economic equilibrium theory of Leontief [28] a static demand-reduction model [16, 29] for n infrastructures is given by:

$$\Delta x = A^* \Delta x + \delta c^*$$

where Δx is the difference between the planned production (x_0) and the degraded production (x_d) production, δc^* is the difference between the planned final demand (c_0) and the degraded final demand (c_d), and A* is a square n × n matrix whose elements a_{ij} (Leontief technical coefficients) represent the ratio of the input from the i-th infrastructure to the j-th one with respect to the overall production requirements for the j-th infrastructure. Starting from [30] and introducing the following transformation [29]:

$$x = [diag\{x_0\}]^{-1} \Delta x = P \Delta x$$

We obtain the static input-output inoperability relation

$$\boldsymbol{x} = PA^*P^{-1}\boldsymbol{x} + Pc^* = \boldsymbol{A}\boldsymbol{x} + \boldsymbol{c} \tag{1}$$

where $\boldsymbol{x}$ and $\boldsymbol{c}$ are the vectors composed, respectively, by the level of inoperability and by the external failure and $\boldsymbol{A}$ is the influence matrix, i.e. the matrix elements a_{ij} of such matrix represent the fraction of inoperability transmitted by j-th infrastructure to i-th one or, in other terms, how much the inoperability of j-th infrastructure influences i-th infrastructure.

The overall inoperability corresponding to a perturbation c is given by:

$$\boldsymbol{x} = (I - A)^{-1}\boldsymbol{c} = \boldsymbol{S}\boldsymbol{c} \tag{2}$$

In the following, let us refer to A and $S = (I - A)^{-1}$ as the open-loop and closed-loop dependency matrices, respectively. Matrix A models the direct effects due to first-order dependencies while matrix S also takes into account the amplifications introduced by domino effects (i.e., second-order and higher-order dependencies). Notice that, under suitable hypothesis of matrix A, of the closed loop dependency matric S can be expressed as

$$S = (\boldsymbol{I} - \boldsymbol{A})^{-1} = \boldsymbol{I} + \boldsymbol{A} + \boldsymbol{A}^2 + \boldsymbol{A}^3 + \cdots$$

Such an equation provides an immediate understanding of the cumulative effects of high-order dependencies in matrix S. i.e. the sum of the direct (first), second, third and so on order of interdependencies.

To quantify the role played by each infrastructure, in [31] the authors introduced the dependency index, defined as the sum of the Leontief coefficients along the single row

$$\delta_i = \sum a_{ij} \tag{3}$$

and the influence gain, i.e., the column sum of the Leontief coefficients

$$\rho_j = \sum a_{ij} \tag{4}$$

Where the first index measures the robustness of the infrastructure with respect to the inoperability of other infrastructures. As a matter of fact, it represents the maximum inoperability of the i-th infrastructure when every other infrastructure is fully inoperable. The lower the value, the greater the ability of the i-th infrastructure to preserve some working capabilities (e.g., using buffers, back-up power, etc.) despite the inoperability of its supplier infrastructures.

On the other side influence gain conversely, measures the influence exerted by one infrastructure over the others. A large influence gain means that the inoperability of the j-th infrastructure induces significant degradations to the entire system.

However, as illustrated in [32] such indices refer only to the direct influence exerted or suffered by each infrastructure. In other terms, those indices do not consider the consequences of second or higher order interdependencies, i.e. the effects induced by multi-step cascading phenomena. These overall effects can be evaluated considering the closed-loop matrix S.

As an example for the IIM, Fig. 4 (left) reports a simplified scenario, which include three infrastructures with the relative influence coefficient and, on the right, the corresponding IIM model.

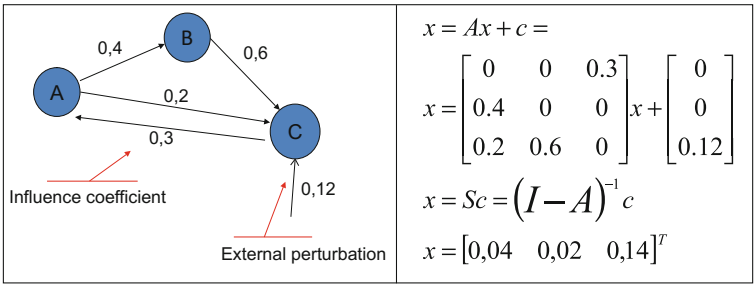


Fig. 4 Example of IIM model for 3 dependent infrastructures

The analysis of the matrix A allows to discover that infrastructure C is the most dependent one with a dependency index of 0.8, while infrastructure A and B are those with the highest influence index $\rho_A = \rho_B = 0.6$.

Equation [2] can be used to estimate, for example, the overall effect of an external perturbation able to reduce the inoperability of infrastructure C of the 12% (i.e. $c = [0 \quad 0 \quad 0.12]^T$). The result $x = [0.04 \quad 0.02 \quad 0.14]^T$ shows that infrastructure A suffers an operability reduction of the 4%, the double of those suffered by infrastructure B, but also that the inter-dependency phenomena exacerbate the negative consequences on the infrastructure C which inoperability level grows up to the 14%.

The static input–output inoperability model defined in Eq. [30] can be extended in the Dynamic IIM (DIIM) by incorporating a dynamic term:

$$\dot{\boldsymbol{x}}(t) = K(A - I)\boldsymbol{x}(\boldsymbol{t}) + K\boldsymbol{c} \tag{5}$$

where $\dot{x}(t)$ represents the variation in the inoperability level at time t and the diagonal matrix normal economic conditions is referred to the industry resilience coefficient matrix because each element k_{ii} measures the resilience of the i-th infrastructure in terms of recovery rate with respect to adverse or malicious events.

The DIIM can be used to analyze the evolution of the inoperability in an inter-dependent scenario until an equilibrium, if any, is reached,[1] as illustrated in Fig. 5 for the example of Fig. 4.

In many application scenarios, however, it is more useful to consider a discrete-time representation of [5]. Given a sampling rate Ts, a discrete time model can be obtained approximating the derivative with the incremental ratio.

$$\boldsymbol{x}(k) = A\boldsymbol{x}(\boldsymbol{k}) + \boldsymbol{c} + \boldsymbol{B}[\boldsymbol{x}(\boldsymbol{k}+1) - \boldsymbol{x}(\boldsymbol{k})] \tag{6}$$

In the case the restoration phase is neglected, i.e. $B = -I$ Eq. [24] simplify in

$$\boldsymbol{x}(k) = A\boldsymbol{x}(\boldsymbol{k}) + \boldsymbol{c}$$

Often for the discrete-time interdependency model one can directly assess the values of the elements of matrix A for example via interview with sectors' experts [33, 32].

The paper of Haimes and colleagues had a large influence and inspired several extensions and particularizations of IIM, which were applied in different contexts to estimate the impact of catastrophic events and major terrorist attacks [29, 34, 35]. However, one needs to note that such models cannot model dependencies at the

[1] An equilibrium condition exists only if the system is stable, i.e. if all the eigenvalues of (I-A) have a strictly negative real part. Notice that the stability of the system does not dependent on the particular matrix K.

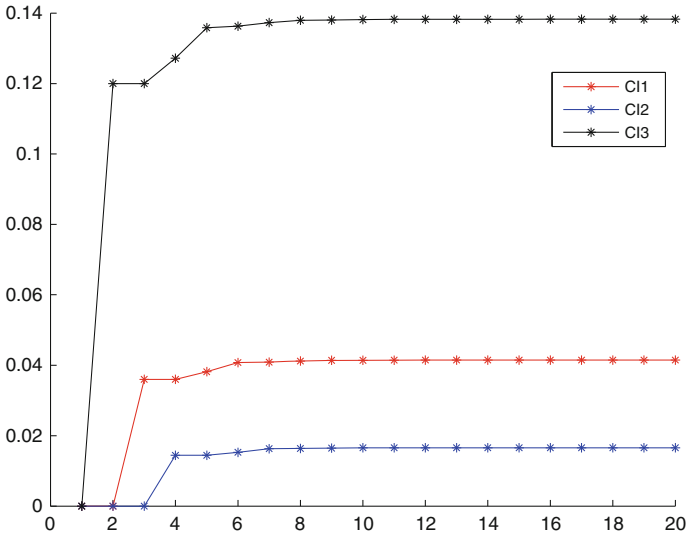


Fig. 5 Evolution of discrete time DIIM for system of Fig. 4

component level, but offer a more macroscopic view. Also, the dependencies identified are derived by normal economic conditions [17].

Similar results can be obtained using System Dynamics (SD) approach. SD is a methodology and a computer simulation modeling technique for framing, understanding, and discussing the dynamic behavior and no-intuitive casual relationships among variables in complex systems. Originally introduced by Jay W. Forrester in the 1960s and used to help corporate managers to improve their understanding of industrial processes [36], SD has been also used in the framework of CI to overcome limits related to the use of past data to predict the future. Indeed, the SD aim to identify individual causalities and how they combine to create feedback loops that are the causes of the counter-intuitive outcomes. It is important to point out that the expected outcomes are not quantitative predictions for a particular variable, but rather a measure of the dynamic behavior pattern of the system, given the inputs and the conditions in the model.

The core of the SD strategy consists in representing the system structure in terms of stocks, flows, and the causal mechanisms that govern their rates of change. Stocks represent quantities or states of the system, the levels of which are governed over time by flow rates between stocks. In SD the dependencies among CI are modelled via two diagrams: causal-loop diagram capturing the causal influence among different variables and stock-and-flow diagram describing the flow of information and products through the system.

Figure 6, for example, presents a causal loop diagram aimed to capture the possible effects of the implementation of policies designed to reduce terrorist acts [37].

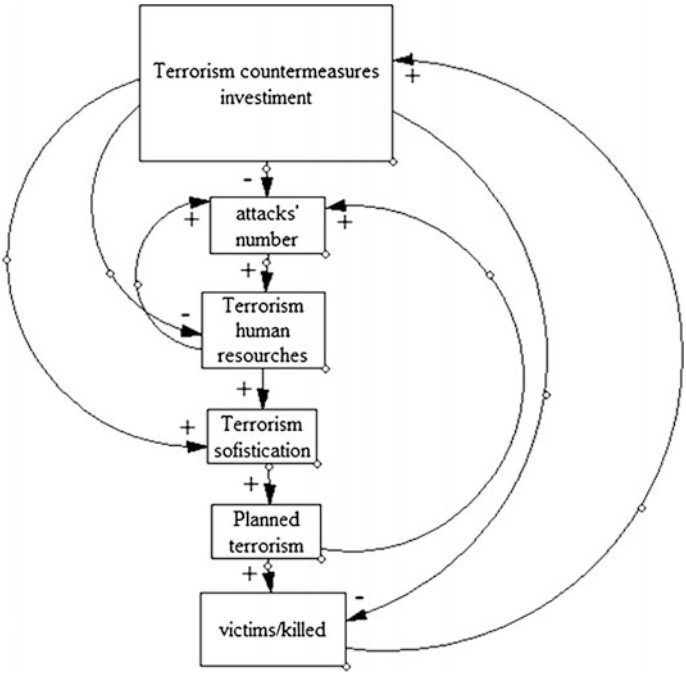


Fig. 6 Example of causal loop diagram of a system dynamic model (modified from [37])

The arrows that link each variable indicate places where a cause and effect relationship exists while the plus or minus sign at the head of each arrow indicates the direction of causality between the variables, when all the other variables (conceptually) remain constant.

The causal diagram shown in Fig. 6 can be interpreted in the following way. As the Government increases its investment in anti-terrorism countermeasures, the number of the perpetrated attacks and the number of terrorist human resources decrease. On the other hand, the anti-government sentiment (as felt by extremist groups) increases. This sparks the hatred extremist groups that use religion, force and/or political causes to obtain resources and recruit more members. Therefore, terrorist human resources (recruitment) increase. As terrorist human resources increase, also terrorist sophistications (strength, lethality and/or capability) increase. And as a consequence, the number of terrorist attacks (planned or not) increases as well. These give a boost to the number of victims, causing the increment, by the Government, of the terrorism-defense resource allocation.

Substantially, SD models the dynamic and the evolutionary behavior of CI scenario trying to capture the most relevant causes and effects relationships under disruptive scenarios. SD allows to include in the model the effects of investments and policy and technique factors to reflect the system evolution in the long term.

SD has been used to perform risk analysis in complex scenarios [38, 39, 33] to analyze the criticality in railway station [40], to improve crisis management in the presence of extreme events [41], so as to design sophisticated tools as CIP/DSS [42].

The main weaknesses of SD is that the causal loop diagram is established based on the knowledge of a subject matter experts. Moreover, being a semi-quantitative method, it use a series of differential equations to describe the system-level behaviors of the CI and this requires the calibration of many parameters and functions in the models, which need a huge amount of data [17].

6 Networked Based Approaches

These approaches try to infer information on dependencies representing the different elements as "nodes" of a network where the presence of a relation between two nodes is depicted via a link connecting them. Their most interesting features are the relative simplicity and the inductivity of the relative assumptions, especially when referred to physical interdependencies. Indeed, the most natural approach is to represent the different components of an infrastructure as the nodes of the network where the links represent their relationship/connection.

Exploiting the powerful toolset provided by graph theory it is possible to characterize the relevance of the different nodes, so as the properties of the whole network [30]. This type of analysis can emphasize that several technological networks due to their peculiar topological structure (generally referred as "scale-free" [43]) are very robust with respect to accidental failure, but at the same time they are very fragile to deliberate attack.

Recently several authors suggested using this approach to analyze also dependency between different CI. In this type of approaches, the physical couplings are mainly considered assuming that the primary source of interdependency is geographical proximity. Here the concept of geographical proximity (that stresses the influence of two nodes in close spatial proximity) embraces, generally, physical and geographical dependencies, as defined by Rinaldi et al. [1].

The underlying idea of these approaches is illustrated in Fig. 7. The figure demonstrates how a perturbation occurred into one graph representing a network is able to influence the properties of another graph representing a second infrastructure (network).

In order to apply such an approach, the researchers have to preliminarily assume:

- *The topological (and eventually dynamic) model of the first infrastructure*, i.e. the nodes and the arcs of the network (and for the dynamic model the flow model to adopt);
- *The topological (and eventually dynamic) model of the second infrastructure*, i.e. the nodes and the arcs of the network (and for the dynamic model the flow model to adopt);

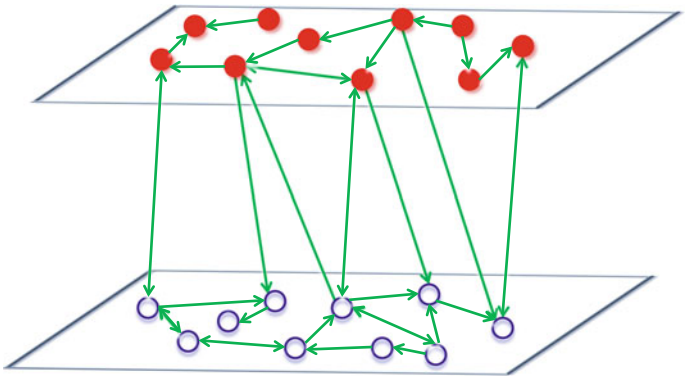


Fig. 7 Topological approaches are based on network-oriented modeling

- *The coupling mechanism existing among the nodes of the two networks*, i.e. how the nodes of the first infrastructure are linked to the ones' of the second infrastructure and vice versa (and for the dynamic model also a threshold mechanism).

Today, the structural vulnerability is one of the most applied tools (see for example [20, 44–48] and the references therein). It is not clear if this is due to the intrinsic importance of such types of relations, or because it is the only approach for which it is feasible to acquire the needed data. However, some authors emphasize that the analysis of structural properties is not able to provide always coherent and exhaustive data.

To overcome such limits, different authors started to consider also the "functional" properties of the network. To this end it is assumed that some form of fluxes "flows" over the networks and it is investigated how a topological event occurred in a network (e.g. the removal of a node or a link) influences the fluxes existing in the other network.

Even if in the literature there are several studies devoted to the functional analysis of a single infrastructure, only recently some studies about coupled infrastructures appeared [19, 49].

The results reported in the literature emphasize how structural and functional vulnerabilities are substantially poorly correlated concepts that capture different properties, i.e. two networks should be strongly coupled from the structural point of view, and at the same time lightly coupled when considering the functional properties and vice versa. Unfortunately, there are no final indications about which one of these properties is the most relevant neither to explain those apparently incoherencies. However, to perform a functional vulnerability assessment, not only is it mandatory to acquire information about the topological structure of the network, but also a model about the characteristics of the fluxes and their specific parameters. This introduces several degrees of freedom into the model that may lead to erroneous conclusions.

In [20] the authors consider the coupling of networks able to reproduce the real structure of a small-scale water and gas networks. They introduce a simple rule to establish interdependencies among networked elements based upon geographical proximity. The work is devoted to investigate, with reference to a set of topological parameters (vertex degree, clustering, characteristic path length, redundancy ratio) the effects of coupling. To this end they introduced a tunable parameter that drives the networks from isolation to complete interdependency.

In [50] it is addressed the problem of interdependent response dividing the problem into analysis of static topological properties, and analysis of the effects of those properties in dynamic response. Dynamic response is investigated through time-dependent properties such as network resilience and fragmentation modes. Using a small-world network model, variation of topological properties as a function of disruption severity is analyzed. Efforts are made to determine if correlations exist among failure models, network component removal strategies, and network topology.

In [21] there is an attempt to formalize the interdependent dynamics among several heterogeneous infrastructures. In this framework a metric for the level of functionality of an infrastructure is given by the sum of the functionality of the infrastructure components divided by the number of components. This approach has been used in [21] to analyze the interconnection of electric grid and telephony network: to investigate the effect, on the telephony network, of removing from the power distribution network one or two nodes, they introduce as metric the remaining fraction of functional telecommunication nodes.

A similar formalism has been proposed in [51] where five types of infrastructure are presented and incorporated into a network flow framework and tested with reference to the lower Manhattan region of New York.

In the framework of functional analysis, an interesting result is proposed in [23] where the interconnection properties of an electric grid and a TLC network that mimic the Italian situation are investigated. The authors used the DC power flow to model the electric flux and developed a specific model to address the packet routing in the TLC network. In this paper the effect of the interdependency is measured in terms of degradation of the QoS (Quality of Service). Specifically, the metric adopted for the electric QoS is the fraction of dispatched power with respect to the nominal load and for TLC the increment in the dispatching time with respect to the unperturbed situation. Then they evaluate how the degradation experimented in the electric QoS affects the TLC QoS.

7 Conclusions

To summarize, all approaches mentioned and analyzed, rely heavily on the availability of high quality data in order to ensure a realistic representation of the CI topology, behavior and failure consequences. In general, this type of data is difficult to obtain and handle either due to their sensitivity or to their volume. Moreover,

there is no standardized data collection methodology for interdependent CI and thus the wider application of such models is hindered.

Even if this data is collected for a first analysis, repeating such an exercise and keeping the data up to date requires significant resources and investments by the industry. Even if in the very last years there is more attention and availability from stakeholder to share data, focusing on approaches that can be easily updated is a significant requirement.

The validation of this type of models is an important step, which is usually neglected, partially due to the lack of real data to test these approaches. Moreover, current models often incorporate theoretical assumptions or abstractions, poses significant challenges when practically applied.

Finally, we observed that the various available methods cover different aspects of the problem and there is the need to combine them in order to battle some of their shortcomings. Integrating or federating models allowing them to exchange data is not a trivial task and we will investigate it further in the following chapters.

Acknowledgement and Disclaimer This chapter was derived from the FP7 project CIPRNet, which has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no. 312450.

The contents of this chapter do not necessarily reflect the official opinion of the European Union. Responsibility for the information and views expressed herein lies entirely with the author (s).

References

1. Rinaldi SM, Peerenboom JP, Kelly TK (2001) Critical infrastructure interdependencies. IEEE Control Syst Mag, 11–25
2. Andersson G, Donalek P, Farmer R, Hatziargyriou N, Kamwa I, Kundur P, Martins N, Paserba J, Pourbeik P, Sanchez-Gasca J, Schulz R, Stankovic A, Taylor C, Vittal V (2005) Causes of the 2003 major grid blackouts in North America and Europe and recommended means to improve system dynamic performance. IEEE Trans Power Syst 20(4):1922–1928
3. Hokstad P, Utne IB, Vatn J (2012) Risk and interdependencies in critical infrastructures. Springer series in reliability engineering. Springer, London
4. Klaver MHA, Luiijf HAM, Nieuwenhuijs AN, van Os N, Oskam V (2016) Critical infrastructure assessment by emergency management. In: CLecture Notes in Computer Science, vol 9568, Springer, Heidelberg, 2016, pp 79–90
5. Barrett C, Beckman R, Channakeshava K, Huang F, Kumar V, Marathe A, Marathe M, Pei G (2010) Cascading failures in multiple infrastructures: from transportation to communication network. In: 5th international conference on critical infrastructure (CRIS), pp 1–8
6. Nieuwenhuijs A, Luiijf E, Klaver M (2008) Modeling dependencies in critical infrastructures. In: Goetz E, Shenoi S (eds) Critical infrastructure protection, IFIP Series, vol 253, pp 205–214
7. Setola R (2010) How to measure the degree of interdependencies among critical infrastructures. Int J Syst Syst Eng 2(1):38–59
8. De Porcellinis S, Panzieri S, Setola R (2009) Modelling critical infrastructure via a mixed holistic reductionistic approach. Int J Crit Infrastruct 5(1–2):86–99

9. Dudenhoeffer DD, Permann MR, Manic M (2006) CIMS: a framework for infrastructure interdependency modeling and analysis. In: Proceedings of the 38th conference on Winter simulation, Dec 2006, pp 478–485
10. Luiijf HAM, Nieuwenhuijs AH, Klaver MHA, van Eeten MJG, Cruz E (2010) Empirical findings on European critical infrastructure dependencies. Int J Syst Syst Eng 2(1):3–18
11. Van Eeten M, Nieuwenhuijs A, Luiijf E, Klaver M, Cruz E (2011) The state and the threat of cascading failure across critical infrastructures: the implications of empirical evidence from media incident reports. Public Adm 89(2):381–400
12. Bologna S, Macdonald R (2002) Advanced modeling and simulation methods and tools for critical infrastructure protection. ACIP Project
13. U.S.-Canada Power System Outage Task Force, "Final Report on the August 14, 2003 Blackout in the United States and Canada: causes and recommendations (2004)
14. Luiijf HAM, Nieuwenhuijs AH, Klaver MHA (2008) Critical infrastructure dependencies 1-0-1. In: First international conference on infrastructure systems and services: building networks for a brighter future (INFRA), 2008, Rotterdam, pp 1–3
15. Aung Z, Watanabe K (2009) A framework for modeling interdependencies in Japan's critical infrastructures. In: Palmer C, Shenoi S (eds) 3rd IFIP international conference on critical infrastructure protection (CIP-2009). Springer, USA, pp 243–257
16. Haimes YY, Jiang P (2001) Leontief-based model of risk in complex interconnected infrastructures. J Infrastruct Syst 1–12
17. Ouyang M (2014) Review on modeling and simulation of interdependent critical infrastructure systems. Reliab Eng Syst Saf 121:43–60. ISSN 0951-8320
18. Macaulay T (2008) Critical infrastructure. CRC Press, Boca Raton
19. Carreras BA, Newman DE, Gradney P, Lynch VE, Dobson I (2007) Interdependent risk in interacting infrastructure systems. In: Proceedings of the 40th Hawaii international conference on system sciences, 2007
20. Duenas-Osorio L, Craig JI, Goodno BJ, Bostrom A (2007) Interdependent response of networked systems. J Infrastruct Syst 185–194
21. Svendsen NK, Wolthusen SD (2007) Analysis and statistical properties of critical infrastructure interdependency multiflow models. In: Proceedings of IEEE workshop on information assurance, pp 247–254
22. Stergiopoulos G, Kotzanikolaou P, Theocharidou M, Gritzalis D (2015) Risk mitigation strategies for critical infrastructures based on graph centrality analysis. Int J Crit Infrastruct Prot 10:34–44
23. Rosato V, Issacharoff L, Meloni S, Tiriticco F, De Porcellinis S, Setola R (2008) Modelling interdependent infrastructures using interacting dynamical models. Int J Crit Infrastruct (IJCIS) 4(1/2):63–79
24. Bologna S, Casalicchio E, Masucci V, Setola R (2008) An integrated approach for simulating interdependencies. In: Papa M, Shenoi S (eds) Critical infrastructure protection II. Springer, Boston, pp 221–231
25. De Porcellinis S, Panzieri S, Setola R, Ulivi G (2008) Simulation of heterogeneous and interdependent critical infrastructures. Int J Crit Infrastruct (IJCIS) 4(1/2):110–128
26. EU project DIESIS (Design of an Interoperable European federated Simulation network for critical Infrastructures), Deliverable "D2.3 Report on available infrastructure simulators" http://www.diesis-project.eu/
27. Pederson P, Dudenhoeffer D, Hartley S, Permann M (2006) Critical infrastructure interdependency modelling: a survey of U.S. and international research. Idaho National Lab, 2006
28. Leontief WW (1951) The structure of the American Economy 1919–1939. Oxford University Press, Oxford
29. Haimes Y, Horowitz B, Lambert J, Santos J, Lian C, Crowther K (2005) Inoperability input–output model for interdependent infrastructure sectors. I: theory and methodology. J Infrastruct Syst 11(2):67–79

30. Albert R, Barabasi A (2002) Statistical mechanics of complex networks. Rev Mod Phys 74:48–97
31. Setola R, De Porcellinis S (2008) A methodology to estimate input-output inoperability model parameters. In: Critical information infrastructures security 2007. Lecture Notes in Computer Science. Springer, Berlin, pp 149–160
32. Setola R, De Porcellinis S, Sforna M (2009) Critical infrastructure dependency assessment using input-output inoperability model. Int J Crit Infrastruct Prot (IJCIP) 170–178
33. Laugé A, Hernantes J, Sarriegi JM (2015) Critical infrastructure dependencies: a holistic, dynamic and quantitative approach. Int J Crit Infrastruct Prot 8:16–23
34. Santos JR (2006) Inoperability input-output modeling of disruptions to interdependent economic systems. J Syst Eng 20–34
35. Santos JR (2008) Inoperability input-output model (IIM) with multiple probabilistic sector inputs. J Ind Manag Optim 489–510
36. Forrester JW (1961) Industrial dynamics. MIT Press, Cambridge, MA
37. Madnick S, Siegel M (2008) A system dynamics (SD) approach to modeling and understanding terrorist networks. Massachusetts Institute of Technology, Cambridge
38. Brown T, Beyeler W, Barton D (2004) Assessing infrastructure interdependencies: the challenge of risk analysis for complex adaptive systems. Int J Crit Infrastruct 1(1):108–117
39. Cavallini S, d'Alessandro C, Volpe M, Armenia S, Carlini C, Brein E, Assogna P (2014) A system dynamics framework for modeling critical infrastructure resilience. In: International conference on critical infrastructure protection, Mar 2014. Springer, Berlin, pp 141–154
40. De Cillis F, De Maggio MC, Setola R (2015) Vulnerability assessment in RIS scenario through a synergic use of the CPTED methodology and the system dynamics approach. In: Railway infrastructure security. Springer International Publishing, pp 65–89
41. Santella N, Steinberg LJ, Parks K (2009) Decision making for extreme events: modeling critical infrastructure interdependencies to aid mitigation and response planning. Rev Policy Res 26(4):409–422
42. Bush B, Dauelsberg L, LeClaire R, Powell D, DeLand S, Samsa M (2005) Critical infrastructure protection decision support system (CIP/DSS) overview. Los Alamos National Laboratory Report LA-UR-05-1870, Los Alamos, NM 87544
43. Albert R, Jeong H, Barabasi A (2000) Error and attack tolerance of complex networks. Nature 406:378–382
44. Bompard E, Napoli R, Xue F (2009) Analysis of structural vulnerabilities in power transmission grids. Int J Crit Infrastruct Prot 2(1):5–12
45. Chopra SS, Dillon T, Bilec MM, Khanna V (2016) A network-based framework for assessing infrastructure resilience: a case study of the London metro system. J R Soc Interface 13 (118):20160113
46. Latora V, Marchiori M (2005) Vulnerability and protection of infrastructure networks. Phys Rev E 71(1):015103
47. Schneider CM, Moreira AA, Andrade JS, Havlin S, Herrmann HJ (2011) Mitigation of malicious attacks on networks. Proc Natl Acad Sci 108(10):3838–3841
48. Zhang Y, Yang N, Lall U (2016) Modeling and simulation of the vulnerability of interdependent power-water infrastructure networks to cascading failures. J Syst Sci Syst Eng 25(1):102–118
49. Kurant M, Thiran P (2006) Layered complex networks. Phys Rev Lett 96:138701
50. Duenas-Osorio L, Craig JI, Goodno BJ (2008) Probabilistic response of interdependent infrastructure networks
51. Lee EE, Mitchell JE, Wallace WA (2007) Restoration of services in interdependent infrastructure systems: a network flow approach. IEEE Trans Syst Man Cybern Part C 37 (6):1303–1317
52. Kröger W, Zio E (2011) Vulnerable systems. Springer, London. ISBN 978-0-85729-654-2
53. Rinaldi S (2004) Modeling and simulating critical infrastructures and their interdependencies. In: 37th Hawaii international conference on system sciences, vol 2, USA. IEEE

54. Zio E, Sansavini G (2011) Modeling interdependent network systems for identifying cascade-safe operating margins. IEEE Trans Reliab 60(1):94–101

Chapter 3
Critical Infrastructure Disruption Scenarios Analyses via Simulation

Mohamed Eid and Vittorio Rosato

Abstract The ultimate target of Modelling and Simulation (M&S) activities in the field of CIP is to provide Models, Methodologies and tools to help in the analysis of different crisis' scenarios and, subsequently, in crisis management decision making. A CIs' disruptions scenario is simply a sequence of random events following a well-defined chronological order. Generally, each identified scenario produces a set of consequences which is a function of: the initiating event, the concerned CIs and the geo-organizational context of the disrupted CIs. Formal sciences represent the reality of our surrounding world. But formal sciences are imperfect and what we call "reality" is the projection of the inaccessible "Reality" on our world. This projection is the only reality we are talking about in formal sciences. Subsequently, formal sciences construct objects in which small parts of the sensible reality are grasped and formalized. These objects can be called "models". We are limiting our interest here to formal sciences and engineering activities that cover both conceptual and phenomenological modelling processes. Models are first validated before being admitted in the construction of a global model of the sensible reality. Regarding our focus on crisis scenarios modelling, simulation and analysis (MS&A), engineers' ambition is to simulate not only independent isolated phenomenon but also interacting multi-physic multi-scale phenomenon.

M. Eid (✉)
Commissariat à l'énergie atomique et aux énergies alternatives,
CEA/DANS/DM2S, CE Saclay, 91191 Gif sur Yvette Cedex, France
e-mail: mohamed.eid@cea.fr

V. Rosato
Computing and Technological Infrastructures Lab, ENEA Casaccia Research Centre,
Via Anguillarese, 301, 00123 S. Maria di Galeria (Roma), Italy
e-mail: vittorio.rosato@enea.it

R. Setola et al. (eds.), *Managing the Complexity of Critical Infrastructures*,
Studies in Systems, Decision and Control 90,
DOI 10.1007/978-3-319-51043-9_3

1 Introduction

The ultimate target of Modelling and Simulation (M&S) activities in the field of CIP is to provide Models, Methodologies and tools to help in the analysis of different crisis' scenarios and, subsequently, in crisis management decision making.

A CIs' disruption scenario is simply a sequence of events following a well-defined chronological order. Generally, each identified scenario produces a set of consequences which is a function of: the initiating event, the concerned CIs and the geo-organizational context of the disrupted CIs. If these consequences represent a significant risk to the citizen safety, society security and or governance continuity, one will talk about a crisis.

The assessment of the consequences of each potential or active scenario of CIs' disruptions results in fundamental pieces of information for robust crisis management and decision making processes.

Having stated the fundamental importance of scenarios assessments, it will be necessary to highlight the major aspects of scenarios simulation and analysis.

2 Scenarios Simulation

The terms "modelling" and "simulation" are differently perceived by the public depending on the field of science, the topic and the context of use.

Formal sciences ultimate target is to represent the reality of our surrounding world. Many philosophers and scientists believe that the reality revealed by science describes only a "veiled" view of an underlying reality that Science can not access. This belief is mainly because of two reasons: formal sciences are imperfect and what we call "reality" is the projection of the inaccessible "Reality" on our world. This projection is the only reality we are talking about in formal sciences. Let's put it in that way: Models and simulation can never reproduce the real "reality". More interesting points of views may be found in [1, 2].

Subsequently, formal sciences construct objects in which small parts of the sensible reality are grasped and formalized. These objects can be called "models". We are limiting our interest only to formal sciences and engineering. That covers both conceptual and phenomenological modelling processes. Models are first validated before being admitted in the construction of a global model of the sensible reality.

Regarding our focus on crisis scenarios modelling, simulation and analysis (MS&A), engineers' ambition is to simulate not only independent isolated phenomena but also interacting multi-physic multi-scale phenomena.

The simulation of well-defined sequences of events in the case of major crises is of great help in:

- Decision making in order to elaborate the best strategies in managing crises and severe accidents.

- Helping operators to prioritize actions in real situation facing systems' primary disruptions and their propagation.
- Helping designers to improve systems' design in view of minimizing disruptions' frequency, disruptions propagation and consequent hazards.
- Training future technical staffs and qualified persons who will be engaged in systems design, systems operation and crisis management.

Developing powerful integrated simulation capabilities is a serious challenge to all scientists and engineers in the field of CIP. This ambition gives birth to two major challenges:

- Developing and validating models considering CIs vulnerability to threats and CIs mutual dependencies.
- Integrating stochastic phenomena in a global coupled modelling process.

We should then understand the disruption of critical infrastructures under the action of a threat, the dependence between CIs disruptions, disruption propagation and their dynamic characteristics.

Towards the understanding of the CIs' disruptions MS&A, let's start by introducing the different types of models.

2.1 Types of Models

Formal sciences recognize four types of models: conceptual, empirical-statistical, logical and qualitative-descriptive models. Brief examples are given in the following.

Conceptual models occupy a large place in formal science R&D activities and cover all domains of scientific investigations, e.g. in:

- Continuum mechanics => Cauchy stress tensor
- Fluid Mechanics => Navier-Stockes Equations
- Heat Transfer => Newton Model
- Material point movement => Newton 3 laws of movement
- Electro-magnetism => Maxwell Equations
- Electrical Circuits => Kirchhoff's Law
- Structure Dynamic => Lagrange's Equations of Motion
- Neutron transports => Boltzmann Equation.

Empirical and statistical models occupy also an important place in formal sciences R&D activities and cover domains such as:

- Rains => Rains flow, distribution and frequencies
- Wind => Wind velocity, direction and frequencies
- Volcano eruptions => Frequencies, released energy and matters
- Fluids mech. => Loss of pressure in Pipes and bents

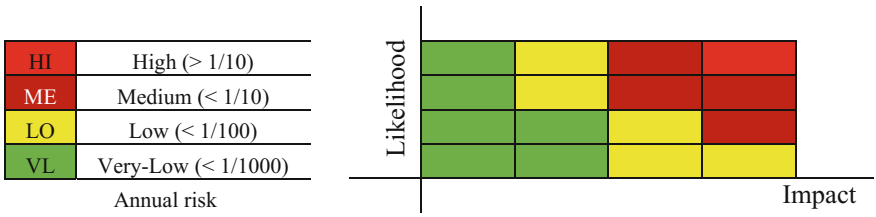


Fig. 1 Flood risk matrix and its color equivalence

- Heat transfer => Radiative heat transfer (Stefan's Law)
- Thermodynamics => Enthalpy and Entropy (p, v, t) curves and tables
- Traffic => Traffic density and Road accidents
- System reliability => Components and Systems Failures
- Diagnosis => Failure detection and monitoring
- Finance => Financial and stock market movement.

Logic and graphical models offer powerful tools to represent logical relationships between systems, functions, actions or concepts and are very used in risk assessments, e.g.:

- Boolean models => Minimal and disjoint cut-sets, critical paths
- Sequential models => Conditional AND gate
- Fault Trees => Static and Dynamic Fault Trees
- Event Trees
- Decision Trees
- Reliability Block Diagrams
- Graphs => networks, states and transitions
- Mind Mapping.

Qualitative and Descriptive models occupy the major place in decision making activities, especially when numerical details do not play an essential role or may muddle up the decision making process. In sever crisis situations, decision makers need only to construct a synthetic view containing only a reduced number of the most vital/strategic parameters to be considered

In Fig. 1, we borrow from [3] the Flood Risk Matrix with a slight modification, as an example of a qualitative-descriptive tools for risk assessment.

The grid shown in Fig. 1 is certainly based on a numerical modelling and assessment. But the final representation of the assessment is given in a qualitative model. The qualitative presentation is synthetic and allows decision makers to grasp the most pertinent information about a given crisis situation.

Certainly, one can't perform algebric operations using qualitative information, in a direct manner.

Having identified the types of models, we should proceed to the identification of the basic elements used in describing crisis scenarios.

2.2 Scenarios' Basic Elements

In order to model, simulate and analyze scenarios of disruptions, one should consider the following elements: the threat action, the CIs' reactions and the consequences.

Threat can be identified and specified by their magnitude and their occurrence likelihood (probability and/or frequency).

The critical infrastructures are described through their vulnerability to the threat action, their mutual dependency and the CIs' disruptions cascading modes and mechanisms.

The consequences describe the impacts of the threat and the CIs disruptions on their environment. Impacts can be of different order: citizen safety, society security, societal moral state, organizational chains rupture, financial losses, assets damage and risk of governance loss of continuity.

The coverage of the above mentioned topics is the ultimate goal of the MS&A activities even if the state-of-the-art in MS&A does not cover satisfactory all three topics: threat, CIs disruption and consequences.

2.3 Identification and Specification of Threats and Consequences

Threat identification and characterization is a first act in any crisis scenario MS&A process. The identification and characterization of threats should necessarily be based on the use of the most appropriate security metrics.

A threats is generally an initiating event that ignites a crisis scenario. Threats are then identified according to their belongings: nature actions, systems disruption and/or man malicious actions. Threats belonging to the category of nature actions are such as: floods, quakes, extreme temperature conditions, hurricanes, tornados, tsunamis etc.… The crisis initiating event can also be originated from industrial systemic disruptions. Industrial systemic disruptions are such as: oil spell accidents, electrical power plants accidents, road (/air/maritime) traffic accidents, chemical and processing plants accidents, power or communication networks' disruptions, financial stock market collapse, human errors etc.… The set of malicious actions covers: criminal actions, vandalism, terrorist actions, etc.…

Once the threat is identified, CIP engineers, end-users and crisis mangers proceed to threat specification. A threat is ideally specified by two figures: its likelihood and its magnitude/strength.

Formally speaking, "likelihood" is a probabilistic measure and can be given in two different metrics: the occurrence probability (dimensionless) or the occurrence rate (per unit time/unit distance/cycle/shock). One can quantify the occurrence probability and the probability rate if historical data are available and have high statistical quality. Otherwise, one uses qualitative metrics such as: certain, highly

probable, probable or rare to qualify occurrence probabilities; and high, moderate or low to describe the occurrence rates. The numbers of considered levels depends on the application type.

The threats are also specified by their magnitudes/strength, such as: the magnitude of an earthquake, the quantity of the rain, the amount of released radioactive substances, the speed of the wind, the rate of water level increase in a flooding river, etc.

Very often, one may uses the term "intensity" to specify threats. One says "an earth quake with high intensity. It causes the death of some hundreds of victims and some thousands of displaced persons".

Using the term "intensity", people refer rather to the impact of the threats and the associated CIs' disruptions. In our methodology, we keep the term "intensity" to measure the consequences of the impact of the threats and the corresponding CIs' disruptions on their environment.

Similar to the double use of metrics (quantitative/qualitative) in specifying the threats, engineers and crisis managers use both kind of metrics (quantitative/qualitative) to specify the consequences (impact) of a given crisis. Consequences can then be measured using different types of natural metrics: number of injuries, fatalities, evacuated persons, destroyed buildings, inaccessible roads, loss of services (transport/water/communication/heating/electricity) and ultimately loss of governance/public unrests.

Once one identified and specified the threat, one still need to know how to model and simulate them.

2.4 Modelling and Simulation of Threats and Consequences

There are two ways for modelling threats and consequences:

- Probabilistic: if data allow, one can develop probabilistic models describing either the occurrence probability functions and/or the occurrence probability density functions. The most commonly used probability density functions are: uniform, exponential, gamma, Gumbel, Gaussian, Weibull …
- Conditional: given a well-defined threat, one determines the corresponding CIs' disruptions and consequences.

Considering one way or the other, analysts should subsequently proceed to the assessment of the disruptions cascade corresponding to the threat that has been identified and specified, above.

2.5 Modelling and Simulation of CIs' Cascade of Disruptions

Cascade of disruptions is widely treated in literature in a very extensive manner and a summary of what was published up to 2009 was assembled by Marhavilas et al. [4].

Generally, we may distinguish two distinct strategies, in MS&A of disruptions' cascade: (1) the agent-based or federated simulation strategy and the pre-established sequences list strategy. Many methodologies are based on a mixed approaches. A detailed screening of the most used or cited methodologies of cascading MS&A are given in the deliverable D2.1 of the EU-PREDICT project report on the state-of-the-art [5].

Focusing on the immediate practical target of this chapter, we have chosen to expose one of the methodologies based on the pre-established scenarios list [6, 7].

But, what is the "cascade of disruptions"?

A crisis scenario is fully described by a given sequence of chronologically ordered CIs' disruptions and produces hazardous impacts on its natural, economic and societal environment.

The CIs implicated in the crisis scenario can be all or in part vulnerable to the threat and mutually dependent. Subsequently, a robust model—describing the cascading of disruptions with the time—should integrate vulnerability and dependency.

2.5.1 Vulnerability

The term "Vulnerability" is used here to describe the dependency between a well-defined threat and the disruption mode and mechanism of a well-defined CI. Obviously, a given CI may show different types of disruption modes depending on the disruption mechanism and the vulnerability of this mechanism to the threat. Also, a CI does not react to all threats in the same manner.

CI disruptions are fundamentally stochastic processes. They can then occur independently from threats, as well. The occurrence of disruptions in the absence of threats will be called "systemic" disruptions. If disruptions are the result of the occurrence of a threat, they will be called "stressed disruptions". Stressed disruptions depend on the vulnerability of the CIs to the stressing threat.

Most of the models describe CIs vulnerability to threats using one the following approaches:

- Qualitative approach; it describes the vulnerability using a qualitative metric such as: extreme vulnerability, vulnerable, medium, low and not vulnerable.
- Binary approach; it describes vulnerability using a binary function [1, 0]. The value 1 means that the CI is vulnerable to the threat, i.e., if the threat happens, the disruption will certainly occur. The value 0 means that the CI is not vulnerable to the threat, i.e., if the threat happens, no disruption occurs.

Table 1 The CI disruption dependency matrix

		Threats			
		Th_1	Th_2	Th_3	Th_4
Impacted disruption	e_1	0	0	2.0	0
	e_2	0.6	0	0	0
	e_3	0	0.8	0	0
	e_4	0	0.2	1.0	0

- Probabilistic approach; it describes in a probabilistic terms the dependency between the threat and the CI disruption. The vulnerability of a given CI "*i*" to a well-defined threat "*j*" will be described using a vulnerability strain factor "υ_{ij}". The disruption rate $\lambda_i(j)$ of a given CI "*i*" under the action of the threat "*j*" will then be given by:

$$\lambda_i(j) = \lambda_i(o)(1 + \upsilon_{ij})$$

where, $\lambda_i(o)$ is the systemic (unstressed) disruption rate of the CI, "*i*", and υ_{ij} is its vulnerability strain factor regarding the threat, "*j*".

If the CI, "*i*", is acted upon by multiple *N* threats, its effective disruption rate $\lambda_i^{N,0}$ will, then, be given by:

$$\lambda_i^{N,0} = \lambda_i(o)\left[\prod_{j=1}^{N}(1 + \upsilon_{ij})\right]$$

where; $\lambda_i^{N,0}$ is the effective disruption rate.

In the presented model, threats act on the same CI, independently. No available models consider the possibility of a compound damage mechanisms. Considering independently the vulnerability to each threat gives a conservative estimation of the effective disruption rate.

The vulnerability strain factor matrix υ_{ij} represents the vulnerability of a disruption mode "*i*" to a given threat "*j*". It describes the increase in the disruption occurrence due to the action of the threat, Table 1.

2.5.2 CI Dependency

The operation of CI depends very often on the operation of some other CIs. One can identify three basic types of dependency:

- Physical/structural,
- Functional/operational,
- Procedural/administrative….

Table 2 The CI disruption dependency matrix

		Impacting disruptions			
		e_1	e_2	e_3	e_4
Impacted disruption	e_1	0	0	0	0
	e_2	0.6	0	0	0
	e_3	0	0.8	0	0
	e_4	0	0.2	1.0	0

In order to count for the possible dependency between CIs, all the available models use a sort of a disruption dependency matrix (D-D matrix). The matrix elements describe the existing mutual dependency between a given set of identified CIs.

Similar to the vulnerability, the description of dependency can be:

- Qualitative,
- Binary, or
- Probabilistic.

The definition of each category is identical to that mentioned above for vulnerability.

The dependency of the disruption of a given CI "*i*" on the disruption of another CI "*j*" is described by a factor ε_{ij} that we will call the CI disruption dependency strain factor. An academic example of the Disruption Dependency (D-D) matrix is given in Table 2.

The disruption rate $\lambda_i(j)$ of a given CI "*i*" given the disruption of the CI "*j*" can then be given as:

$$\lambda_i(j) = \lambda_i(o)(1 + \varepsilon_{ij})$$

where, $\lambda_i(o)$ is the systemic (unstressed) disruption rate of the CI, "*i*", and ε_{ij} is the dependency strain factor regarding the disruption of the CI, "*j*".

A disruption dependency is called "directional" if the disruption of the CI "*j*" impacts on the disruption of the CI "*i*", while the inverse is not true. Then, one has $\varepsilon_{ij} > 0$ and $\varepsilon_{ji} = 0$.

If the disruption dependency is not directional, we will talk about "interdependency" rather than "dependency" and have, generally, $\varepsilon_{ij} \neq \varepsilon_{ji} > 0$.

An illustrative example of the independence strain matrix ε_{ji} is given in Table 2.

If the CI, "*i*", is acted upon by multiple disruptions of other *M* CIs, its effective disruption rate $\lambda_i^{0,M}$ will, then, be given by:

$$\lambda_i^{0,M} = \lambda_i(o)\left[\prod_{j=1}^{M}(1 + \varepsilon_{ij})\right]$$

where, $\lambda_i^{0,M}$ is the effective disruption rate.

In the presented model, the disruptions of many CIs act independently on a given CI. We have not considered the possibility of a compound damage mechanisms. Considering independently the impact of each other disruption gives a conservative estimation of the effective disruption rate.

2.5.3 Integrating Vulnerability and Dependency

In a complex case, where there are many disrupted CIs and simultaneously multi-threat actions, the overall effective disruption rate $\lambda_i^{N,M}$ will be given by:

$$\lambda_i^{N,M} = \lambda_i(o)\left[\prod_{k=1}^{N}(1+\upsilon_{ik})\right]\left[\prod_{j=1}^{M}(1+\varepsilon_{ij})\right]$$

where N refers to the number of the simultaneous acting threats and M refers to the number of the already disrupted CIs.

2.6 *Cascading of Disruptions*

Disruption cascading can be described by the occurrence of some discrete and independent disruptions e_i that happen in a well-specified order $[e_1 \rightarrow e_2 \rightarrow e_3 \cdots \rightarrow e_n]$. The corresponding occurring instants are defined by $[t_1, t_2, t_3, \ldots, t_n]$, where $[t_1 < t_2 < t_3 < \cdots < t_n]$, [7]. Each of these instances $[t_1, t_2, t_3, \ldots, t_n]$ has its distribution probability function (pdf), $\rho(t)$. The first disruption event is e_1 and the last is e_n.

The probability $p_n(t)$ that cascading T happens within the interval [0, t] is given by:

$$p_n(t) = \int_0^t \rho_1(\xi_1)d\xi_1{}^* \int_{\xi_1}^t \rho_2(\xi_2)d\xi_2{}^* \ldots{}^* \int_{\xi_{n-1}}^t \rho_n(\xi_n)d\xi_n \qquad (1)$$

This integral can be solved numerically for most of the pdf $\rho_i(t)$ and analytically if the pdf $\rho_i(t)$ is of Poisson type.

The pdf $\rho_i(t)$ can be determined if one has a conceptual mathematical model describing the CI disruption. The probability density function $\rho_i(t)$ and the occurrence rate $\lambda_i^{N,M}$ are correlated. Knowing one of them allows to determine the other.

Otherwise, the occurrence rate $\lambda_i^{N,M}$ can be determined if we have enough data in the CI disruption databases. It is one of the reasons why disruption databases and crisis databases are very important issues for MS&A of CI.

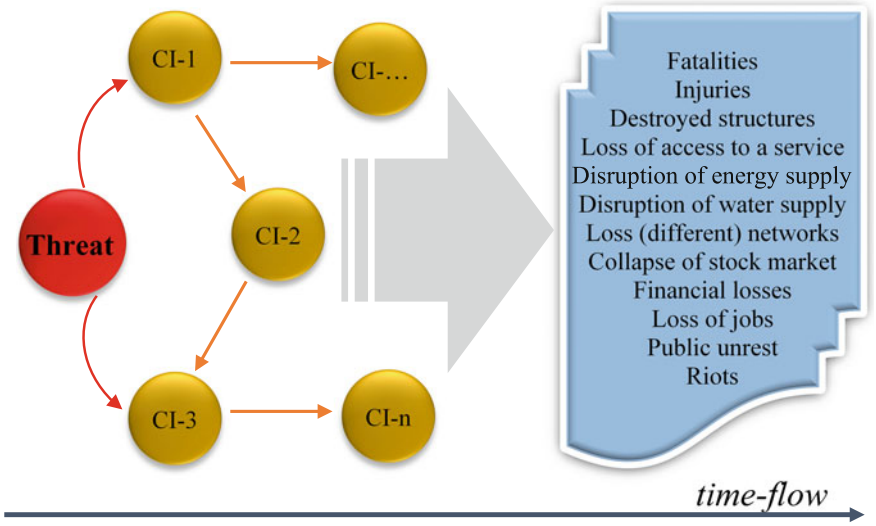


Fig. 2 A schematic representation of the full story line-time

The databases issue touches the determination of the systemic disruption rates, the stressed disruption rates, the vulnerability strain factor and the dependency strain factor.

2.7 The Story Time-Line

The cascade is then build up on the time-line with three distinguished phases: active threat, CI-disruptions considering vulnerability and dependencies and finally consequences. However, these three phases are not sequential on the time-line. They can be overlapping. Although, the CI's cascade of disruptions is built up of sequential disruptions, Fig. 2.

3 A Hypothetical Crisis Scenario

The major target of this chapter is to illustrate how the MS&A of the cascade of disruptions provides critical input data to the decision making and crisis management.

A hypothetical scenario, but inspired form real, will be considered in the following to illustrate the methodology of simulating and analyzing crisis scenarios. We recall that one should: identify and specify the thread(s), identify the concerned CIs, determining their respective vulnerability to the thread(s), specify the CIs'

Table 3 Threat magnitude-vulnerability equivalence grille

	Catastr.	Extreme	Strong	Medium	Low	Insignificant
$(1+\upsilon)$	>10	10–6	6–3	3–2	2–1	1–0

mutual dependency, identify the crisis scenario(s) (cascading of disruptions) to be assessed.

Each identified cascading of disruptions lead to a pre-identified set of consequences (hazardous impacts). The likelihood of yielding a given set of consequences is proportional to the likelihood of the occurrence of the corresponding scenario.

3.1 Crisis Scenario Description

Consider an aging dam, regulates the flow of a river using a large retention lac behind and has 2 water alarm levels: alarm-level-1 (AL-1) and alarm-level-2 (AL-2).

If the water level attends AL-1 in the retention lac, a nearby water pumping station starts up automatically to evacuate the water excess to a small emergency retention area far from the lac. It is a provisional evacuation in order to stabilize the water at level AL-1 or below.

The pumping station is supplied by electricity from the national grid. In case of grid supply loss accident, a local supply electrical unit (a large diesel generator) can be immediately activated.

If the water level in the retention lac attends level AL-2, the risk of losing the dam's structure integrity becomes significant. A major Crisis is publicly declared and the population in the area should be evacuated within 24–36 h.

3.2 Identification and Specification of the Threat

The threat is a combination of an extreme heavy rain and a river flood.

The combination of both threats considered having a strong magnitude on a magnitude scale compromising 6 levels: catastrophic, extreme, strong, medium, low and insignificant.

The vulnerability of the concerned CIs' disruption will depend on this magnitude through the vulnerability strain factor υ, Table 3.

The number of levels on the magnitude scale and their corresponding numerical values has no standard rules. It can change in function of the threat and the considered CIs with their geographical-societal context. Very often, it is defined by mixing approaches from: experience feedback and expert judgement.

Table 4 Systemic occurrence rate of the disruption modes

	D. mode #1	D. mode #1	D. mode #1	D. mode #1
$\lambda_{systemic}$	1e−4	5e−3	2.5e−2	1.25e−1

Table 5 The dependency strain factors

		Impacting disruptions			
		d_1	d_2	d_3	d_4
Impacted disruption	d_1	0	0	0	0
	d_2	0	0	0	0
	d_3	0	0.8	0	0
	d_4	0	0.4	0.4	0

The levels of magnitude and their equivalence in strain factors, given in Table 3, are for the academic illustration.

3.3 Identification and Specification of the CIs and Their Vulnerability

The hypothetical crisis scenario compromises four CIs each shows a specific unique disruption mode. Disruption modes are specified by their systemic occurrence rates, λ, respectively.

The systemic occurrence of a given disruption mode is a random event. It occurs whether the threat is active or not and whether the disruption mode is dependent on other disruption modes or not. Certainly, we consider the case of coherent disruption modes, i.e., the action of threats and the interdependency on other disruption modes cant but increases the considered occurrence rate.

Considering the above magnitude-vulnerability equivalence grille, in Table 4, and supposing that the impact of the threat is similarly moderate on the considered four disruption modes. The vulnerability strain factor υ will be taken equal to 1.5, i.e., the systemic occurrence rate of each disruption mode will be multiplied by a factor equal to 2.5.

3.4 Specification of the CIs Dependency

The dependency between the four considered disruption modes are given, in Table 5, below. As one can recognize, both disruption modes d_3 and d_4 are moderately dependent on d_2. While, the d_4 shows also a dependency on d_3 disruption mode.

3.5 Definition of the Cascade of Disruptions

The following cascade of disruptions is identified as one of the possible scenarios that may lead to a serious crisis. It is defined by the occurrence of the four specified disruption modes in the following order, (d_1, d_2, d_3, d_4), while:

- Disruption d1: loss of the electricity supply from the grid to the pumping station.
- Disruption d2: loss of the evacuation capability (loss of the water pumping station). [It covers the loss of the emergency local electrical supply (a large diesel unit), the loss of automatic start up system and other systemic mechanical failure modes of the pumping unite.]
- Disruption d3: loss of the dam structure integrity. [It covers all cracks with sizes larger than a critical value and/or the full collapse of the structure.]
- Disruption d4: loss of the capability of population evacuation. It covers: the failure of the population alert systems (media and SMS), the unavailability of the emergency resources, the loss of accessibility to the evacuation meeting points and the loss of transportation capabilities. [It includes systemic, humans and organizational failure modes.]

3.6 Definition of the Crisis Management Target

The crisis management target is to **evacuate at least 99% of the population in the disaster zone within the interval 24–36 h from the crisis declaration starting moment**.

The crisis starts when the water level in the lac behind the dam reaches the AL-2.

3.7 The Consequence to Mitigate or to Dump

We consider that the crisis is successfully managed if: at least 99% of the concerned population can be evacuated after 36 h from crisis starting moment.

There is evidently a no-zero risk not to succeed in achieving this target.

The unique hazardous consequence to be considered is “having a non-evacuated population rate higher than 1% after 36 h from crisis starting moment”.

3.8 Scenario Assessment: Simulation and Analysis

For the sake of our illustrative purpose, we limited our assessment to only two levels of simulations:

- Simulation #1: assessing the likelihood of a systemic occurrence of the identified cascading of disruptions. A systemic occurrence supposes no threat's actions and no dependencies. The CIs are called unstressed.
- Simulation #2: one considers the threat's actions (vulnerability strain factors non-null) and the dependencies between disruption modes (dependency strain factors non-null). The CIs are called stressed.

3.8.1 Whey the Unstressed Case?

The unstressed case represents a kind of a background crisis. A crisis that we can live with, even unhappily. If we do not accept its likelihood level, we should change the whole system: CIs, operating modes, environment, organization and/or the acceptable level of likelihood. This background crisis serves as a referential to assess the likelihood of the crisis when the CIs are stressed by the action of the crisis active vectors.

Again and for the sake of our illustrative purpose, the likelihood of the crisis in both situations (stressed and unstressed) is assessed using only metrics vectors: the occurrence probabilities and the occurrence rates.

The time profiles of the occurrence probability and of the occurrence rates are assessed over a period of time equal to 80 h starting from the moment when the water level behind the dam attends the alarm-level-2. We use the time interval to reach 90% of the asymptotic occurrence probability as a characteristic figure. The 90% of the asymptotic occurrence probability will be called the reduced asymptotic probability (RAP) and the time to attend it is called TTA-RAP. Theoretically, the asymptotic values are attended when $t \rightarrow \infty$ which is not a practical measure in taking decisions.

Regarding the occurrence rates, we use the most probable value of the occurrence rate (MPR) as a characteristic figure and the time to attend it will be referred to as TTA-MPR.

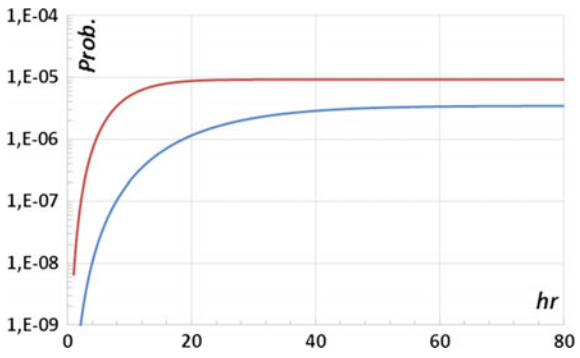


Fig. 3 Occurrence probability time-profile for the unstressed (*blue*) and stressed (*red*) CIs

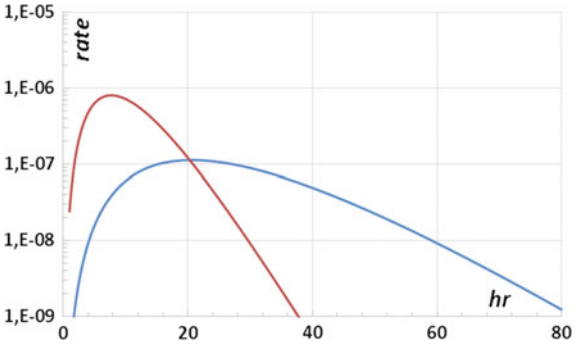


Fig. 4 Occurrence rate time-profile for the unstressed (*blue*) and stressed (*red*) CIs

Table 6 The classification of the criticality according to the occurrence rate

Cat.	Likelihood	Occurrence rate	Time interval (hours)	
			Case #0	Case #4
1	Low	$\leq 10^{-8}$	0 – ~4 h 60 – ∞ h	30 – ∞ h
2	Medium	$10^{-8} - 10^{-7}$	4 – 15 h 27 – 60 h	0 – 2 h 20 – 30 h
3	High	$\geq 10^{-7}$	15 – 27 h	2 – 20 h

Table 7 The occurrence probability and the occurrence rate characteristics

	As. prob.	RAP	TTA. RAP (h)	MPR	TTA MPR (h)
Case #0	3.46e−6	3.11e−6	44	1.13e−7	20
Case #4	9.25e−6	8.32e−6	17	8.00e−7	7.8

3.8.2 Unstressed Case

The CIs are not vulnerable to the threat and the CIs' are not dependent. The likelihood of this cascade of disruptions is the following:

- The occurrence probability of the cascade is time dependent. It attends the RAP value of 3.15e−6 after 46 h, Fig. 3.
- The occurrence rate of the cascade is also a time dependent function. It attends its MPR value 1.13e−7 after 21 h, Fig. 4.

The systemic occurrence of this cascade of disruptions may result inacceptable consequences. Therefore the crisis managers would be interested in identifying the likelihood of the situation and its evolution with the time. Assessing this risk-background is useful in measuring the "time criticality" for deciding and acting during the crisis, as will be explained in the following.

Given that the most probable value of the cascade occurrence rate, the background risk-noise, is about 10^{-7} and occurs around 21 h, one may propose the following classification based on three classes, Tables 6 and 7:

- Class 3—high: the occurrence arte is almost one decade around the most probable value of the noise risk [$>10^{-7}$]. This is the case between 4 and 60 h from the start of the active phase of the threat.
- Class 2—medium: the occurrence rate is one decade less than in class 1, [10^{-8}, 10^{-7}]. This is the case in two intervals: from 1 to 4 h and from 60 to 85 h.
- Class 1—low: the occurrence rate is one decade below class 2, [$<10^{-8}$]. This is the case before 1 h and after 85 h, in the unstressed case (background-risk).

The unstressed case services in establishing the scale of criticality to be used in assessing the stressed cases representing crisis situations. Four hypothetical crisis situations are presented in the following.

3.8.3 Stressed Case

All disruptions $[d_1, d_2, d_3, d_4]$ are equally vulnerable to the threat and have vulnerability strain factor equal to 1.5. The threat is considered of moderate magnitude similar to case #2. Dependencies between disruptions are considered. Disruptions d_3 and d_4 show dependency on d_2 and their dependency stress factors are 0.8 and 0.4, respectively. Disruption d_4 show dependency on d_3 with a dependency stress factor equal to 0.4 [$\varepsilon_{32} = 0.8, \varepsilon_{42} = 0.4, \varepsilon_{43} = 0.4$]. A comparative synthesis is given in Tables 6 and 7:

- The occurrence probability of the cascade is time dependent. It attends its RAP value of 8.32e−6 after 17 h, Fig. 3.
- The occurrence rate of the cascade is also a time dependent function. It attends its MPR value of 8.00e−7 after 7.8 h, Fig. 4.

The occurrence probability is higher than in case #0 (and all the other cases). Its dynamic behavior is faster than in case #1 but of the same order as the three other cases.

4 Conclusions

Based on a dynamic model describing the cascade of disruptions, a methodology is proposed to measure the criticality of time to take decisions and actions in crises situations.

A methodology is proposed and can briefly be described as based on:

- The vulnerability and the dependency are taken into account in the disruption occurrence rate.

- Disruptions are stochastic events. Subsequently, a well-defined sequence of disruptions may occur even in the absence of the threat action and the dependency between CIs. That is called a systemic cascade and it occurs even when the corresponding CIs are unstressed.
- The dynamic of systemic cascade is used as a referential dynamic for all possible stressing modes resulting from the same well-defined cascade of disruptions.
- The dynamic of a cascade (stressed and unstressed) is characterized by its occurrence probability and its occurred rate and their time-evolution profile.
- The occurrence probability is used to measure the cascade likelihood.
- The occurrence rate time-profile is a good measure of the cascade dynamic. It is used to measure the time-criticality regarding decision and action making.

Using exact dynamic models to assess cascade reveals some interesting effects:

- The likelihood of a given cascade does not necessarily increasing with the threat intensity, in spite of the individual increase of the likelihood of the disruptions composing the cascade.
- Schematically, higher are the threat magnitude/strength and/or the CIs dependency, faster goes the dynamic of the cascade.

Acknowledgement and Disclaimer This chapter was derived from the FP7 project CIPRNet, which has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 312450.

The contents of this chapter do not necessarily reflect the official opinion of the European Union. Responsibility for the information and views expressed herein lies entirely with the author(s).

References

1. Hennig C, (2009) Mathematical models and reality—a constructivist perspective. Research report No.304, Department of statistical science, university college london, June 2009. http://www.ucl.ac.uk/statistics/research/pdfs/rr304.pdf
2. Byl J, (2003) Mathematical models and reality. In: Proceedings of the 2003 conference of the association for christians in the mathematical sciences
3. Pitt M, (2008) A comprehensive review of the lessons to be learned from the summer floods of 2007. Final report, June 2008. http://webarchive.nationalarchives.gov.uk/20100807034701; http://archive.cabinetoffice.gov.uk/pittreview/_/media/assets'; www.cabinetoffice.gov.uk/flooding_review/pitt_review_full%20pdf.pdf

4. Marhavilas PK, Koulouriotis D, Gemeni V (2011) Risk analysis and assessment methodologies in the work sites: on a review, classification and comparative study of the scientific literature of the period 2000–2009. J Loss Prev Process Ind 24(2011):477–523
5. PREDICT Consortium, D2.1—State of the art of the R&D activities in cascade effect & resilience and global modelling. EU-PREDICT project, REDICT-20151218-D2-1/V3
6. Eid Mohamed et al (2016) Critical infrastructure preparedness: cascad-ing of disruptions considering vulnerability and dependency. J Pol Saf Reliab Assoc—Summer Saf Reliab Semin 7(1–2):2016
7. Eid M (2011) A general analytical solution for the occurrence probability of a sequence of ordered events following poison stochastic processes. J Reliab Theor Appl RT&A # 03 2(22) (ISSN 1932-2321, Electronic journal of international group on reliability, registered in the library of the USA congress)

Chapter 4
Physical Simulators of Critical Infrastructures

Antonio Di Pietro, Carlo Liberto, Nikolas Flourentzou, Elias Kyriakides, Ivo Pothof and Gaetano Valenti

Abstract Critical Infrastructures are an essential asset in modern societies and our everyday life is heavily dependent on their reliable and secure operation. The problem of controlling and managing critical infrastructures is becoming more and more difficult as they are increasing in size due to the growing demand for the services they provide and the geographical spread required. As these infrastructures become larger and more complex, fewer people understand how these networks work and the interactions between all the components. Thus, models are necessary so as to accurately predict their behavior under steady state or under failure/attack scenarios. This chapter provides a review on modeling and simulation approaches of critical infrastructures and in particular of electric power, telecommunications, water supply and drainage systems, and transportation systems.

A. Di Pietro (✉) · C. Liberto · G. Valenti
ENEA, Laboratory for the Analysis and Protection of Critical Infrastructures and Laboratory of Sustainable Mobility, Rome, Italy
e-mail: antonio.dipietro@enea.it

C. Liberto
e-mail: carlo.liberto@enea.it

G. Valenti
e-mail: gaetano.valenti@enea.it

N. Flourentzou · E. Kyriakides
Department of Electrical and Computer Engineering and KIOS Research Center for Intelligent Systems and Networks, University of Cyprus, Nicosia, Cyprus
e-mail: flourentzou.nikolas@ucy.ac.cy

E. Kyriakides
e-mail: elias@ucy.ac.cy

I. Pothof
Department of Industrial Hydrodynamics, Deltares, Delft, The Netherlands
e-mail: Ivo.Pothof@deltares.nl

R. Setola et al. (eds.), *Managing the Complexity of Critical Infrastructures*, Studies in Systems, Decision and Control 90,
DOI 10.1007/978-3-319-51043-9_4

1 Introduction

Critical Infrastructures (CI) are the assets, systems, and networks, whether physical or virtual, which are essential for the functioning of a society and economy. Typical examples of critical infrastructures are electric power systems, telecommunication networks, water supply systems and transportation systems. These are dynamic, large-scale, complex, spatially distributed and data-rich systems. CI in urban areas deteriorate at an unknown pace, especially water, urban drainage and gas networks. Moreover, the damage to one of these systems, their destruction or disruption by natural disasters, terrorism, criminal activity or malicious behaviour, may produce a significant negative impact for the security and the wellness of citizens and being exacerbated by the existence of dependencies among different infrastructures [1]. For instance, an outage occurring in an electrical distribution network can produce disruptions for the telecommunication services which in turn may alter the normal functioning of banking services in a specific area thus causing negative effects for the citizens.

As CI are aging, interactions need to be accounted for in risk-based design, operation and management. However, many failure mechanisms associated with CI interactions are still poorly understood. To support the preparedness capability of CI managers and decision makers such as Civil Protection operators, modeling and simulation across CI has recently become a key field of study. For example, in pre-event times, an electric operator can run a power flow simulator on its power grid model to verify the feasibility of specific load shedding actions. Moreover, a water supply operator can simulate the behavior of its water network and verify management strategies for improving the water quality throughout the network. During post-event times, simulators may be used to implement allocation policies or resources (e.g., electricity, water) or to improve response readiness of emergency transportation facilities such as fire engines, fire trucks, and ambulances to reach the disaster areas.

In several EU countries the pace with which infrastructure is rehabilitated implicitly assumes that the technical lifetime is between 120 and 800 years. Clearly this is unrealistic. Due to ageing, the functionality gradually decreases, while the underlying processes and interactions between individual infrastructures are largely unknown. This, combined with a growing pressure on these infrastructures (climate change, 82% of the population in EU living in urban areas by 2050), is requiring to increase our understanding of all processes involved along with the development of engineering tools for (re-)design.

There are several ways that can be utilized to model critical infrastructures, including network flow models, system dynamics models, agent-based models, or combinations of these models. These modeling methodologies are used in commercial or research-based "physical simulators". These are tools that try to mimic the behaviour of a system. They can be deterministic or stochastic, continuous time or discrete-time based or being based on differential or software agents. In this chapter, the focus is on simulators that can reproduce the behavior of the major

critical infrastructures by analyzing the kind of data they require and produce and thus on the benefits they can provide to the different end users.

This chapter provides a summary of some of the main tools used for modeling critical infrastructures. Clearly, the list is non-exhaustive as there is a large number of commercial or research-based physical simulators in use today.

2 Power Systems

At the epicenter of the well-being and prosperity of society lie the electric power systems. Contemporary power systems are operated under heavily stressed conditions due the ever increasing electricity demand and deregulated electricity market. Maintaining the reliability and security of the power systems under such stressed conditions is challenging. The occurrence of severe faults and disturbances in the system needs to be detected timely, and necessary actions need to be taken.

In order to prepare for faults or unexpected load changes, power system operators assess the stability of the power system by examining offline several scenarios. The transient analysis that is usually used in the power system control center enhances the situational awareness of the power system operators by providing a visualization of the generator rotor angles, bus voltages, and system frequency during large contingencies. Therefore, operators can plan a set of remedial measures to maintain the stability of the system.

The electrical power system is typically divided in three main sections: the Generation in large power plants, the long distance Transmission network, and the Distribution grid. There are several software applications which study the power system and its multitude of components. Some of the most used physical simulators for power systems are described in this Section.

2.1 DIgSILENT PowerFactory

PowerFactory [2] is a solution for modelling and analysis of generation/transmission/distribution/industrial grids, overall functional integration, and data management. It offers a complete suite of functions for studying large interconnected power systems integrating new technologies for power generation and transmission such as wind generation, virtual power plants, HVDC-VSC or FACTS. PowerFactory's functions can be applied to improve the security, stability and economics of complex power transmission systems.

PowerFactory provides comprehensive modelling features for studying all kinds of phasing technologies, meshed or radial topologies and railway supply systems connected to public distribution systems. In order to reduce network unbalance, improve quality of supply and optimize distribution networks, PowerFactory offers

multi-phase power flow analysis, short circuit analysis (IEC 60909, ANSI C37 and multiple fault analysis), harmonic analysis, time-domain simulation and reliability assessment. Other standard features include the modelling of distributed generation and virtual power plants, voltage drop analysis, branch loading calculation, daily load curves and the consideration of LV load diversity. This is complemented by an easy-to-use protection coordination wizard.

Industrial power systems supplying refineries, paper-mills, car factories or other plants with high power quality requirements benefit from high precision PowerFactory power flow algorithms, short circuit calculation features, four-wire modelling, harmonics-analysis and filter design options.

PowerFactory can also be used for analyzing the impact of distributed generation on the network. It combines classical distribution system analysis functions, such as voltage drop calculation, unbalanced network, load and generation modelling, and selectivity analysis.

DIgSILENT StationWare provides a reliable central protection settings database and management system for the complete power system substation data, both to manage the various control parameters and to centrally store substation related information. StationWare is based on the latest .NET technology.

DIgSILENT PowerFactory Monitor (PFM) is a multi-functional Dynamic System Monitor which fully integrates with DIgSILENT PowerFactory software. The PFM features grid and plant monitoring, fault recording, grid characteristics analysis by offering easy access to recorded data, analysis of trends, verification of system upset responses and test results.

2.2 SIEMENS PSS® E

PSS E is a fully-featured software for electrical transmission system analysis and planning. It provides integration into clients' workflow (through built-in Python® API) for automation and customization. PSS E provides comprehensive modeling capabilities for enabling sophisticated analyses and accuracy. It anticipates network problems and analyzes alternatives. It calculates the area exchanges in the power network planning. PPS E is used by transmission planners, operations planners, consultants, and research communities.

PSS® MOD is used for Project Modeling and Data Management, which is specifically designed for PSS E. The user can manage a great number of change cases for PSS E. PSS MOD assembles sets of model changes into "queues". Queues can then be managed and organized in various fashions depending on the needs of the PSS E user. Queues are coupled with PSS MOD seasonal and annual profiles to provide the PSS E user with a procedure for organizing and reorganizing system investigations. All this without the need for generating a great number of PSS E base cases, or repeatedly rerunning PSS E cases when planning sequences change.

2.3 SIEMENS PSS® SINCAL

The SINCAL platform offers a full set of calculation modules based on a single database "all-in-one", and optimized GUI for specific tasks. SINCAL is used for the complete simulation and easy evaluation based on commercial databases, for real-time simulation, for the management of protection devices, and for workflow-driven system planning.

SINCAL provides a complete range of modules for design, modeling and analysis of electrical power systems as well as pipe networks; gas pipes for calculations for different pressure levels, water pipes for steady-state, dynamic and water tower filling calculation, and district heating and cooling pipes for calculation of flow and return flow.

SINCAL offers a comprehensive range of analysis modules and tools facilitating the planning, design and operation of power systems. Its field of application ranges from short-term to long-term planning tasks, fault analysis, reliability, harmonic response, protection coordination, stability (RMS) and electromagnetic transient (EMT) studies.

SINCAL supports all types of networks from low to the highest voltage levels with balanced and unbalanced network models e.g., four wire systems or transposed systems with the full coupling matrix. It can be used for cost analysis of future scenarios as well. Several analysis modules, such as protection or dynamic simulation, are also ideally suited for training purposes.

2.4 SIEMENS PSS® NETOMAC

NETOMAC is designed as a single program for facilitating access to and manage tasks associated with the dynamic phenomena of electrical power networks. It links up the most important methods for the analysis of dynamics of electrical networks in the time and frequency domains. The NETOMAC key features of the tool offer:

- Simulation of electromagnetic and electromechanical transient phenomena in the time domain and frequency range analysis;
- Steady-state load-flow and short-circuit current calculations;
- Optimization and eigenvalue analysis;
- Real-time simulation for protection testing, network security calculations;
- Simulation of torsional vibration systems;
- Parameter identification and reduction of passive/active networks;
- Interactive network training simulator and extended user interface for the graphical input of network and controllers structures and results documentation;
- Data import from other planning packages (e.g. PSS® E, PSS® SINCAL) and additional formats for data export.

The NETOMAC program system presents a multitude of possibilities for simulating all electromagnetic and electromechanical phenomena in electrical systems. The analysis in the frequency domain usefully supplements the processing possibilities. The eigenvalue analysis opens up numerous methods leading further, such as the establishing of dynamic, reduced network models by reducing the order.

Many kinds of pre-processing are available, such as parameterizing of power lines or motors and identifying of model parameters. The possibilities of system analysis are supplemented by user-defined optimizing processes.

NETOMAC links up the most important methods for the analysis of dynamics of electrical networks in the time and frequency domain. It is a program for all tasks associated with the dynamic phenomena of electrical networks. It presents real-time capability for protection testing and network security calculations thus providing fast response when network problems occur.

2.5 MATLAB® Simulink®

Simulink is a block diagram environment for multidomain simulation and Model-Based Design. It supports system-level design, simulation, automatic code generation, and continuous test and verification of embedded systems. Simulink provides a graphical editor, customizable block libraries, and solvers for modeling and simulating dynamic systems. It is integrated with MATLAB, enabling to incorporate MATLAB algorithms into models and export simulation results to MATLAB for further analysis.

Simulink is used by industry, research communities, for real-time experimental verification and for educational purposes.

Key Features

- Graphical editor for building and managing hierarchical block diagrams;
- Libraries of predefined blocks for modeling continuous-time and discrete-time systems;
- Simulation engine with fixed-step and variable-step ODE solvers;
- Scopes and data displays for viewing simulation results;
- Project and data management tools for managing model files and data;
- Model analysis tools for refining model architecture and increasing simulation speed;
- MATLAB Function block for importing MATLAB algorithms into models;
- Legacy Code Tool for importing C and C++ code into models.

2.6 PowerWorld Simulator

PowerWorld is an interactive power system simulation package designed to simulate high voltage power system operation on a time frame ranging from several minutes to several days. The software contains a power flow analysis, voltage control, generation control and area interchange, contingency analysis, linear sensitivity analysis, and fault analysis.

The Simulator includes the following features:

- Intuitive, User-Friendly GUI
- Model Explorer
- Solutions Options
- Presentation Tools
- Interactive, Animated Diagrams
- Contingency Analysis
- Geographic Information Systems
- Time-Step Simulation
- Automated Diagram Creation and Modification Tools
- Compatibility
- Modeling Capabilities
- Sensitivities
- Area Generation Control
- Difference Flows
- Contoured Displays
- Script Actions
- Customer Support

PowerWorld is a tool for system planning and operation technicians, engineers, electricity market analysts and managers involved in power system network analysis. It is used by the energy industry to enhance the customer experience. It is also suited for research and teaching power systems operations and analysis.

2.7 PSCAD™ EMTDC™

PSCAD is time domain simulation software for analyzing transients in electrical networks. It can simulate control systems and complex networks by managing data in a completely integrated graphical environment. It solves differential equations of the power system and controls in the time-domain. The results are computed as instantaneous values in time but can be converted to phasor magnitudes and angles by the true RMS meters and/or FFT spectrum analyzers.

PSCAD is a collection of programs, providing a graphical Unix-based user interface to electromagnetic transients program. EMTDC is an integral part of

PSCAD as it is the library of power system component models and procedures, which establish the simulation software provided with PSCAD.

EMTDC (with PSCAD) is used by engineers and scientists from utilities, manufacturers, consultants, and research/academic institutions, all over the world. It is used in planning, operation, design, commissioning, tender specification preparation, teaching, and advanced research.

PSCAD performs evaluation of switching transients and harmonics generated by static converters and analyze over-voltages, instabilities and non-linearities in a power system. It examines transient effects of distributed generation and Sub-Synchronous Resonance.

E-Tran is a software program which gives additional capabilities to PSCAD. It allows a direct translation of Power System Simulator data into PSCAD, while the complete model can be represented graphically. It has data entry based on the same per-unit system and data entry standards as used in loadflow programs. An E-Tran add-on (which allows large PSCAD cases to be broken up and run using parallel processing on multiple cores or on multiple computers) achieves significant reduction of the simulation runtime.

2.8 EMTP-RV

EMTP is a computational engine for the simulation and analysis of electromagnetic, electromechanical and control systems transients in multiphase electrical power systems. It can be used to investigate grid integration of wind generation units, and to analyze and control power electronics for power systems. EMTP provides solutions to coordinate insulation for large networks. It provides protection features associated with power oscillations and saturation problems. It analyzes ferroresonance, shaft torsional resonance stress, and studies synchronous machines control and excitation.

EMTP is used by the industry, engineers and research communities, and for educational purposes to give a first experience on the simulation and analysis of power systems transients.

3 Telecommunication Networks

Telecommunication simulators can be used to verify analytical models, evaluate the performance of new protocols, or to test the security of the networks against cyber attacks. Most of them are based on the Discrete Event Simulation (DES) engine and allow to model the behaviour of a network (e.g., a local area network or LAN) by calculating the interaction among components (e.g., hosts, routers, data links, packets). When a virtual network component is used in conjunction with live

applications and services, this mechanism is also referred as network emulation. In the following, we focus on ns-2, the most common network simulator that targeted at networking research. Further, we list the main functionalities of other simulators.

3.1 ns-2

ns-2 [3] is a public domain event-driven network simulator developed at UC Berkeley. It is available on different platforms such as UNIX, Free BSD and Windows OS platforms. ns-2 provide simulation tools including result display, analysis and converters to simulate small-scale networks.

It can simulate of a variety of IP networks and applications such as (TCP and UDP implementation, traffic source behaviour such as FTP, Telnet, Web, CBR and VBR, router queue management, routing algorithms such as Dijkstra and multi-casting and some MAC layer protocols for LAN). ns-can accept three different languages to code the network: (i) Tcl, which is used to write simulation scripts; (ii) OTcl, to define the event-scheduler and indicate the traffic sources when the traffic starts and stops; and (iii) C++, to implement the schedulers and network components.

Figure 1 shows Nam, an animation tool for viewing network simulation traces and real world packet traces that can be used to analyze ns-2 based network evolution through a simulation. Nam supports topology layout, packet level animation, and various data inspection tools.

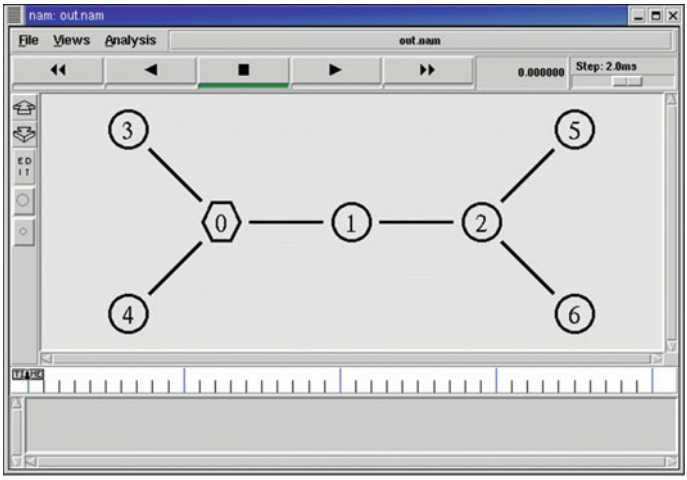


Fig. 1 Simulation topology

3.2 Other Simulators

OMNET++ [4] provides a set of high-level communication protocols and provide additional features to develop complex IT systems, queuing networks or hardware architectures. OMNET++ includes: (i) a graphical network editor (GNED) to allow graphical topology build; (ii) a simulation kernel library containing definitions of objects used to create topologies; (iii) a compiler for the topology description language; (iv) a Graphical and command-line interfaces for simulation execution; (v) Graphical tools for results analysis; (vi) a model documentation tool to create dynamically documentation on the created model.

iSSFNet [5] network simulator relies on common API for parallel simulation of networks, the scalable simulation framework (SSF). Based on iSSFNet, a network viewer module of the simulation environment (RINSE) allows to have different views of the simulated network as well as to execute commands such as attacks and defenses commands and try specific countermeasures to preserve the services delivery of the network.

OPNET [6] allows the analysis and design of a communication network, the devices, protocols, and applications used. OPNET allows to analyse simulated networks to compare the impact of different technology designs on end-to-end behaviour and incorporates protocols and technologies. In addition, it includes a development environment to model specific network types and technologies including VoIP, TCP, IPv6, etc.

4 Water Networks and Urban Drainage

The following phases are recognized in the life cycle of a pipeline system (see also the Dutch standard NEN-EN 3650 ‘Requirements for Pipeline Systems’): (i) Design; (ii) Construction and commissioning/testing and (iii) Operation and maintenance (O&M).

Before the design, the development stage takes place, also known as the preliminary design. The preliminary design is mostly determined by the usage requirements (functional requirements) and planning aspects. The design phase can be divided into the basic design and the detailed design.

In the basic design, the definite points of departure (schedule of requirements) for the design are determined. In the detailed design, the calculations, drawings and specifications are established for the realisation and operational management stage. There is no clear distinction between the two design stages and, in this section, it is summarised as ‘design’. The design of water infrastructure is an iterative process consisting of the pipeline design/network layout, design of pumping stations and other main components, design of surge protection devices and control strategies and finally the design of monitoring instrumentation and incidental O&M procedures [7]. Iterations in these design steps may be required for various reasons. For example, the

surge protection may become so expensive that a slightly larger pipe diameter or other pipe routing may lead to a more LCC-effective system. Another reason for iterations in the design steps is the fact that the engineering team needs to find a balance between conflicting criteria, such as a short residence time in a drinking water network, leading to selection of small diameter pipes, versus minimum pumping costs, leading to larger pipe diameters. The final system design is affected by many of these conflicting technical and non-technical criteria.

Physical simulators are mainly used to support the iterative decision processes during the design and O&M phase of water supply and urban drainage systems. Physical simulators are used to a lesser extent during the construction/commissioning phase. The overall fundamental objective of using physical simulators for water infrastructure is to support decision making to obtain an acceptable serviceability level at acceptable societal life cycle costs. One could start a philosophical discussion on replacing the words 'acceptable' by 'minimum', but I have chosen 'acceptable' on purpose. The subsections hereafter will address the main topics for which physical simulation tools are used in these three life cycle phases.

4.1 Design Phase

Physical simulators serve different but very similar purposes for drinking water infrastructure and urban drainage infrastructure, as illustrated in Table 1 hereafter. Furthermore, this table summarises what kind of simulator functionality is required to verify the specific design criterion.

Table 1 shows that physical simulators can be used at three different time scales. The basic lay-out of the infrastructure can be determined with steady state modeling approaches, while most detailed design questions demand for so-called extended period or slow transient simulations spanning typically one or two days. Simulation at these time scales can be applied to large distribution networks, including all pipe components down to the level of the individual property owner. Most of the simulation models, addressing this time scale, can be transferred from the design phase to the O&M phase and are being used in day-to-day operations of the water infrastructure.

The full transient simulation models include pressure wave propagation phenomena in pressurized systems. Full transient models are computationally much more expensive that slow transient models. These models are used for a wide variety of emergency conditions and have typical simulation time horizons of a few minutes up to 24 h, depending on system size and design question. It is generally not necessary to run a full transient model on a complete all-pipe network lay-out, although the current computing power is getting strong enough to do so.

Since the water infrastructure is getting more and more automated to save energy and other operational costs, the design of normal control systems is verified in more detail nowadays than a couple of decades ago. The design of these control systems needs to be evaluated in full transient mode, because the pressure wave propagation

Table 1 Overview of design criteria and physical simulator requirements for water infrastructure

Generic design criterion	Water supply	Urban drainage	Physical simulator functionality
Hydraulic capacity	Design flow demand distribution. Max flow rate	Maximum stormwater run-off. Max. domestic inflow in separated system	Steady state
Pressure, Water level	Normal operating pressures within limited range, typically 2–6 barg in distribution networks	Water levels below ground level (no flooding) and no combined sewage overflow for regular run-off conditions	Slow transient
Water quality	Residence time acceptable, chlorine concentration (if applicable)	Limited residence time to limit biological decay. Sufficient local velocities for solids transport	Slow transient
Extreme pressures during emergency conditions	Power failure, Emergency valve closure, start/stop procedures, etc.	Power failure in pressured wastewater systems	Full transient
Robust automation	Emergency control systems, normal control settings	Sewerage networks generally have very limited controls, but pressurised wastewater systems have similar complexity as water supply systems w.r.t. control	Full transient

in pressurized (waste) water networks interferes with the operation of the control systems [8]. Furthermore, emergency control systems are used in combination with anti-surge hardware and may reduce investment costs for the anti-surge hardware significantly [9]. Similar simulators are not only used for the hydraulic design of the water networks and transmission systems, but also for the hydraulic design of treatment facilities [10].

Physical simulators of water infrastructure are used as a verification tool to test whether all applicable criteria are accomplished. Many simulators have built-in optimization routines to further support the design and decision processes, for example to select optimized pipe diameters or to find a minimum required surge vessel volume that satisfies the transient criteria on minimum pressures and water levels.

4.2 Construction and Commissioning Phase

Most of the water infrastructure is built with trenched installation techniques, for which physical simulators are not required. Very dedicated simulation tools are being applied for specialized installation techniques such as horizontal directional drilling (HDD).

The commissioning phase of water infrastructure, especially large pumping stations, can be supported with physical simulators, especially in situations in which the design scenarios cannot be clearly replicated during site acceptance tests (SAT). Many practical issues may lead to deviations between design and commissioning. Two examples are listed: (1) A new pumping station connected to an existing network; (2) a new wastewater pumping station which is designed for a certain future flow rate, which cannot be delivered immediately after construction. In these situations, the commissioning can be performed with temporary system modifications to accommodate the design flow or the commissioning can be performed under part-load conditions. Both approaches for the commissioning phase need physical simulators for model calibration and for extrapolation of commissioning results to design scenarios. Physical simulators, typically full transient models, are also used to set-up the commissioning tests in situations where temporary system modifications are required to perform site-acceptance tests.

4.3 Operation and Maintenance (O&M) Phase

The physical simulators that have been for design are used in the O&M phase as well in a similar off-line mode. Typical activities which are supported by physical simulators include:

(1) Redesign of existing infrastructure;
(2) Debottlenecking to mitigate a performance loss;
(3) Temporary modifications to support maintenance operations (e.g. flushing of a drinking water network, replacing pipe sections in a water network, etc.);
(4) Troubleshooting to analyze incidents, like a water quality complaint or pipe burst.

An emerging field is the real-time coupling of physical water infrastructure simulators to the existing SCADA systems. In this way, the simulation model is used as an advanced and spatially detailed instrument to measure the primary processes in the water infrastructure. Such a model will be helpful for troubleshooting activities, since the real-time model performance can be analyzed after an incident has occurred. Furthermore, if the model is calibrated in an automatic way, performance loss can be detected in an early stage. The real-time integration of measurements and physical modeling results, combined with clear performance indicators has proven to be very valuable for the operation and maintenance scheduling of complex pressurized wastewater networks [11].

These kind of model-data integration applications are necessary for the further development of Model-Predictive-Control (MPC) strategies in water supply and urban drainage applications. Historic data analyses are widely used in the operational control of water distribution networks and urban drainage systems. MPC is the next step to further improve the performance of the existing water infrastructure.

It is anticipated that physical simulators at different temporal and spatial scales will be required for MPC applications.

Finally, other simulation tools are used to support decision making on replacement, refurbishment or renovation works [12, 13]. So far, these Asset Management simulation tools have not been included, since the focus of this section was on the primary processes and not on deterioration processes of the infrastructure and its surroundings.

5 Transportation Systems

Overall concept

Urban street networks are increasingly susceptible to unplanned disruptions triggered by extreme natural phenomena or man-made emergencies including traffic accidents of high severity. Efforts to address this challenging issue, leading to high social and economic losses, are needed to increase network ability to absorb the consequences of disruptions in the face of adverse events.

There is thus a pressing need to assess network vulnerability, that is to understand how a street network and its functionality might be impacted when subjected to disruptions [14, 15, 16]. Vulnerability measures based on distance are more suitable for sparse regional networks since drivers may need to take longer detours to reach their destinations in case of link disruption [17]. By contrast, in dense urban network where many alternative routes may be available drivers often prefer quicker routes which need not necessarily be shorter in terms of distance. For this reason, time-based approaches to studying vulnerability are more appropriate in high traffic density urban areas.

Vulnerability analysis provides valuable insights to facilitate the development of suitable responses to possible crisis situations and to properly prioritize investments for developing network resistance to disruptions. Basically, each component of a network contributes with a different weight to the vulnerability of a network and that weight could change through time, within a day or day-by-day, mostly due to travel demand fluctuations.

Immediately after a network disruption, drivers are forced to explore the network and modify their travel behavior according to their travel experience and reliance on the available information sources. The main options that the drivers can do are to change their normal route, to postpone their trips, to switch to alternative travel modes or to satisfy needs at other destinations.

However, the modeling of driver reaction to major network disruptions presents some methodological challenges, both in describing the day-to-day route choice process and in assessing its confidence and compliance with received information to adapt its behavior. A further modeling difficulty comes from the extensive and expensive data collection efforts needed to capture attitudes and perceptions that shape their day-to-day travel decisions.

In scientific literature, many studies have been conducted to identify and evaluate weakness points of a network, where link closures are likely to occur, and where the impacts would be the most severe. Some analytical approaches have been proposed to find structural weaknesses in the network topology, neglecting network-wide impacts on travel demand in terms of congestion and negative externalities [18–22].

Further approaches have been conducted by using traffic assignment technique that allows to simulate how Origin-Destination (OD) travel demand loads the links of a network when road closures occur [15, 16, 23].

An OD Matrix is traditionally determined through the costly procedure of conducting OD travel surveys in the study area usually conducted once in every one decade and by the time the survey data are collected and processed, the OD data obtained become obsolete. Alternatively, an OD matrix can be estimated by using traffic counts on links and prior OD flow estimations to guide the solution procedure.

Traffic simulation models have also become a useful tool for studying how candidate alternate routes can accommodate traffic diverted when disruptions occur. Current simulation techniques range from microscopic models, capturing the behavior of vehicles and drivers in much more detail thus providing a more comprehensive representation of the traffic process, to macroscopic models tending to model traffic of large networks, in lesser detail, as a continuous flow often using formulations that are inspired by gas-kinetic or hydrodynamic equations.

Traffic simulation models can also be broadly categorized as static and dynamic models. The former focuses on long-term, steady traffic states, while the latter focuses on short-term, dynamic traffic states. Compared to static models, dynamic traffic models have a more realistic representation of traffic flow, and a more detailed representation of the traffic system.

However urban traffic networks are usually really complex systems with a large number of vehicles, many road sections and intersection points often with conflicting traffic flows which can result in a large amount of congestion. Consequently, only sophisticated dynamic simulators are well suited to urban environments where demand greatly varies over time and large fluctuations in travel times occur as a result of congestion, queues that build up and dissipate, and so on. Furthermore calibrating a complex traffic simulator is time-consuming process that requires extra care to adjust capacity, demand, and behavior parameters so that field-observed traffic data can be well-approximated.

In the following, we analyze in detail an analytical simulation tool called FIRST (TraFfic AnalysIs in EmeRgency Situations Tool) to model and measure vulnerability within dense urban networks, to estimate the impact area caused by traffic disruptions and to determine possible diversion routes around the closed streets.

A key novelty of our simulation tool is that we use a large amount of Floating Car Data (FCD) to derive, in a cost-effective way, the travel and traffic patterns in a urban area in terms of OD relations, route choice information, congestion levels and

travel times. Our framework thus combines topological properties of a network, including basic traffic rules, with patterns of road usage and OD locations of the drivers throughout a day extracted from FCD. FIRST uses a comprehensive street network database including geometry and attributes that are needed to identify sound traffic diversion strategies around disruptions. FIRST utilizes heuristic approaches to estimate the OD of the traffic on the closed links and to reassign the estimated OD to the remainder of the network to find alternate routes for traffic diversion.

The vulnerability metrics and the simulation of disruption scenarios was applied to the case of the street network of Rome using FCD collected by an extensive sample of privately owned vehicles currently reaching a penetration rate of around 8%.

Description of the traffic simulator

FIRST is a software tool designed to assist decision makers in strengthening urban street network resilience against traffic disruptions triggered by extreme natural phenomena or man-made emergencies including traffic accidents of high severity. FIRST has a module that incorporates analytical approaches to measure street network vulnerability through the calculation of criticality indicators. The module is aimed at measuring the amount of deterioration in the network functionality caused by the partial or total closure of network components within a reference time period.

The approaches combine the structural properties of the street network with traffic demand patterns at different times of day and locations. Each criticality index is estimated by generating a number of shortest paths connecting two nodes extracted according to time dependent OD patterns. Two different types of criticality indicators are estimated: “Centrality” and “Importance”. Centrality indicator depends on the number of Shortest Paths passing through an arc. The effect of removing an arc from the network is considered by the Importance indicator that measures the average increase of travel time produced by the removal of a specific link. Therefore links with high Importance values guarantee an efficient network functionality as its removal causes a significant growth of travel time.

FIRST includes a multi-step preprocessing module to convert raw FCD into a suitable form for detailed traffic and travel analysis. Floating car data are collected by fleets of privately owned vehicles equipped with an on-board unit that stores GPS measurements (position, speed, direction of movement and signal quality).

The preprocessing module is focused on correcting or removing the possible measurement errors caused by failures in the tracking device, reconstructing OD trajectories from sparse sequences of consecutive GPS traces and finally determining the most likely route in the network by matching sequences of positioning data into a street digital map. The map-matching algorithm implemented into the preprocessing module to infer the route traveled by vehicles is really important not only for extracting OD relations between zones and analyzing travel route choice behavior but also for providing travel time data for network performance evaluation and extracting useful traffic patterns such as vehicle turning rates at intersections, origin and destination locations of vehicles moving on a street or congestion levels

on network elements, including variations within a day and between weekdays and weekends. Map-matching is also a key process to identify the complex spatial-temporal dependencies between links which are particularly relevant to discover congestion propagation patterns resulting from disruptions.

The occurrence of emergency that disrupts the normal flow of traffic necessitates diversion and routing operations to effectively limit traffic demand approaching the blocked streets. FIRST contains useful modules aimed at supporting the estimation of the impact area around the blocked streets, that will form the search space to find alternative routes, and the identification of upstream intersections potentially affected by queue spillbacks and congestion occurring after disruptions.

FIRST incorporates a module to determine possible diversion routes around the closed streets. This module consists of a two steps approach. The first step involves the OD matrix estimation for the vehicular traffic on the closed links derived from the sample of floating vehicle trajectories crossing the closed streets in the time period of disruption. In the second step the module performs the reassignment of the estimated OD Matrix to the remainder of the network in order to find viable diversion routes, starting and termination points of diversion and critical intersections along each alternative route where changes in traffic signal timing may need to be done to accommodate additional diverted traffic flows.

FIRST processing modules, implemented in Java to ensure platform independence, are accessible through a WebGIS application developed in a complete Open Source environment, including the database PostreSQL and its spatial extension "PostGIS", to facilitate advanced geo-spatial queries and map model results.

The test site of ROME

FIRST modules have been applied and tested to estimate the vulnerability of Rome street network, to examine the effects of traffic disruption and to identify effective traffic diversion strategies. Three different information layers are used: a digital street network database containing topological and functional data of each component, a digital map database of census blocks to design traffic analysis zones and an extended collection of travel data generated by a large fleet of privately-owned vehicles while moving in the study area.

The Tele Atlas MultiNet map database of Rome (Fig. 2) is used in our study as it offers a highly accurate reproduction of the street network including current road attributes, speed restrictions and traffic conditions. The database contains a directed graph with 205.567 nodes and 432.405 arcs.

Each road segment contains several attributes on the functional road class, the direction of traffic flow (one-way, two-way, divided highway), the number of running lanes, the traffic free flow speed, the restricted maneuvers, etc. Among these attributes we pay special attention to "Net2Class" classification because it defines the role that a particular network segment plays in serving traffic flows through the network. Furthermore, there is a relationship between posted speed limits and functional classification.

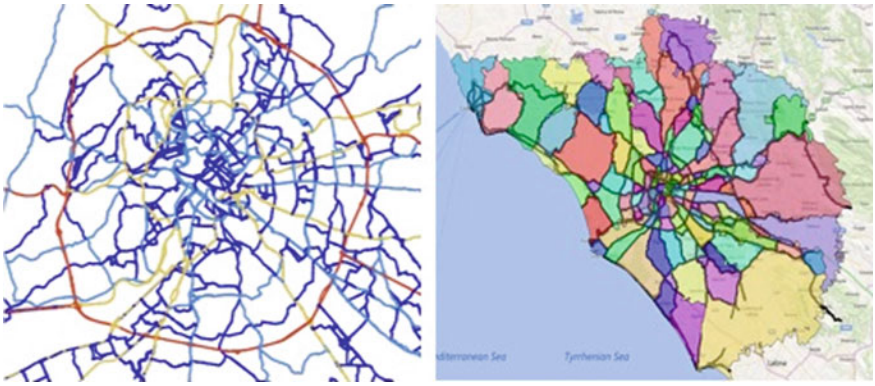


Fig. 2 *Left* Rome MultiNet graph up to Net2Class = 3. *Right* Area zoning outcome

The hierarchical properties of the urban street network are exploited in our approach to restrict the estimation of criticality indexes to major arterial that are designed to provide long-distance movements although shortest path computation is run on the whole street network. After this, we subdivide the study area into 136 Traffic Analysis Zones (TAZs) (Fig. 2) in order to establish the basis from which to estimate Origin-Destination (OD) matrices representing travel demand at a given time window.

A monthly collection of geo-referenced data from an extended fleet of privately owned vehicles traveling within the metropolitan area of Rome has been used. Vehicles are equipped with a tracking device remotely controlled by a software platform operated by OCTOTelematics (http://www.octotelematics.com/en), a company that provides telematics services for insurance companies, car rental and fleet management. From the given collection of about 150×10^6 GPS traces we have extracted approximately 12×10^6 trajectories representing the trips made in Rome by all the equipped vehicles during May 2013.

Vehicle trajectories have been grouped on the basis of the day of the week and six time slots (0–6, 6–9, 9–12, 12–16, 16–20, 20–24) in order to estimate OD matrices for each group. Thus each OD matrix element represents the percentage of trips that flow from a origin TAZ to another destination TAZ in a specific day of the week and a given daily time slot.

Figure 3 shows the criticality maps for the urban street network of Rome. These represent a very useful and intuitive tool for city planners and other decision makers in order to prevent problematic situation and address efforts to solve them.

In Fig. 4, the simulated effects from the temporary closure of a central square (Piazzale Flaminio) and the suggested diversion routes around the closed streets are plotted.

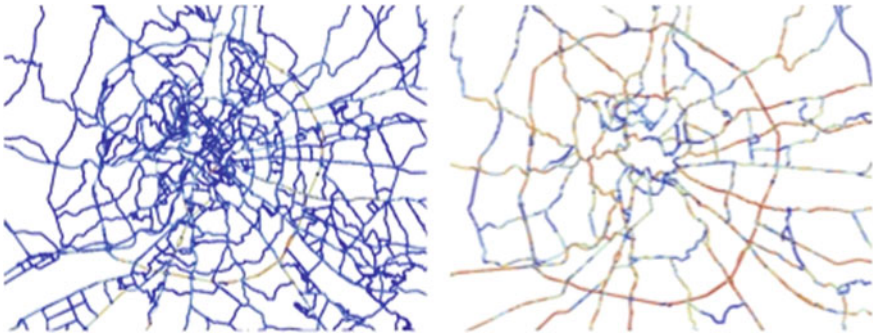


Fig. 3 *Left* Stress Centrality Map over 6 am to 9 am Mondays. *Right* Importance Map over 6 am to 9 am on Mondays

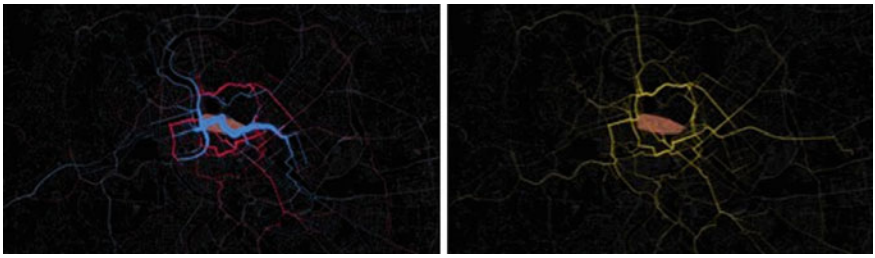


Fig. 4 *Left* Simulated traffic disruptions map. *Right* Diversion routes map

6 Conclusions

In this paper, we provided an extensive description of the modeling and simulation tools used to design and analyze large infrastructures i.e. electric power, telecommunications, water supply and drainage systems, and transportation systems. We showed how simulators can be useful in different phases of the analysis of the behavior of an infrastructure and become an effective means to operators to test several scenarios.

Acknowledgement and Disclaimer This chapter was derived from the FP7 project CIPRNet, which has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 312450.

The contents of this chapter do not necessarily reflect the official opinion of the European Union. Responsibility for the information and views expressed herein lies entirely with the author(s).

References

1. Kyriakides E, Polycarpou M (eds) (2015) Intelligent monitoring, control, and security of critical infrastructure systems, studies in computational intelligence. Springer, Berlin
2. Gonzalez-Longatt F, Rueda JL (2014) PowerFactory applications for power system analysis, 1 edn. Springer International Publishing (ISSN: 1612–1287)
3. McCanne S, Floyd S ns–network simulator. http://www-mash.cs.berkeley.edu/ns/
4. Varga A (2001) The OMNeT++ discrete event simulation system. In: Proceedings of the European simulation multiconference (ESM'2001)
5. Liljenstam M, Liu J, Nicol D, Yuan Y, Yan G, Grier C (2005) Rinse: the real-time immersive network simulation environment for network security exercises. In: Workshop on principles of advanced and distributed simulation
6. OPNET (2012) OPNET network simulation tools. http://www.opnet.com (accessed 2013)
7. Tukker M, Kooij CK, Pothof IWM (2013) Hydraulic design and management of wastewater transport systems (CAPWAT Manual), Deltares. ISBN 978-94-91099-12-0. http://capwat.deltares.nl
8. Pothof IWM, Karney B (2012) Guidelines for transient analysis of supply systems. In: Ostfeld A (ed) Water supply system analysis—selected topics, InTech—OpenAccess Publisher, ISBN: 978-953-51-0889-4. http://www.intechopen.com/books/water-supply-system-analysis-selected-topics
9. Zwan S, van der Alidai A, Leruth PH, Pothof IWM (2015) Integration of emergency control systems in the anti-surge design of large transmission schemes. In: Proceedings 12th international conference on pressure surges, 18–20 Nov 2015, Dublin, Ireland, pp 557–565
10. Alidai A, Pothof IWM (2014) Guidelines for hydraulic analysis of treatment plants equipped with ultrafiltration and reverse osmosis membranes. Desalin Water Treat. doi:10.1080/19443994.2014.979244
11. Kooij C, Muhle S, Clemens FHLR, Pothof IWM, Blokzijl FH (2015) Performance indicators for complex wastewater pumping stations and pressure mains. In: 1st international conference on industrial networks and intelligent systems (INISCom), 2–4 March 2015, Tokio, Japan, pp. 94–99
12. van Riel W, van Bueren E, Langeveld J, Herder P, Clemens F (2016) Decision-making for sewer asset management: theory and practice. Urban Water J 13(1):57–68. doi:10.1080/1573062X.2015.1011667
13. Cook DM, Boxall JB (2011) Discoloration material accumulation in water distribution systems. J Pipeline Syst Eng Pract 2(4):113—122
14. Berdica K (2002) An introduction to road vulnerability: what has been done, is done and should be done. Transp Policy 9(2):117–127
15. Mattsson LG, Jenelius E (2015) Vulnerability and resilience of transport systems—a discussion of recent research. Transp Res Part A Policy Pract. Available online 19 June 2015, ISSN 0965-8564, http://dx.doi.org/10.1016/j.tra.2015.06.002
16. Murray AT, Grubesic TH (2007) Critical infrastructures, reliability and vulnerability. Springer, Berlin
17. Jenelius E, Petersen T, Mattsson L-G (2006) Importance and exposure in road network vulnerability analysis. Transp Res Part A 40(7):537–560
18. Demšar U, Špatenková O, Virrantaus K (2008) Identifying critical locations in a spatial network with graph theory. Trans GIS 12(1):61–82
19. Jiang B, Claramunt C (2004) Topological analysis of urban street networks. Environ Plan 31:151–162
20. Newmann M (2010) Networks: an introduction. Oxford University Press, Inc., New York, NY, USA
21. Porta S, Crucitti P, Latora V (2006) The network analysis of urban streets: a primal approach. Environ Plan 33:705–725

22. Strano E et al (2013) Urban street networks, a comparative analysis of ten European cities. Environ Plan 40(6):1071–1086
23. Nicholson A, Du Z-P (1997) Degradable transportation systems: an integrated equilibrium model. Transp Res Part B 31(3):209–223

Chapter 5
Phenomenological Simulators of Critical Infrastructures

Alberto Tofani, Gregorio D'Agostino and José Martí

Abstract The objective of this chapter is to introduce and discuss the main phenomenological approaches that have been used within the CI M&S area. Phenomenological models are used to analyse the organizational phenomena of the society considering its complexity (finance, mobility, health) and the interactions among its different components. Within CI MA&S, different modelling approaches have been proposed and used as, for example, physical simulators (e.g. power flow simulators for electrical networks). Physical simulators are used to predict the behaviour of the physical system (the technological network) under different conditions. As an example, electrical engineers use different kind of simulators during planning and managing of network activities for different purposes: (1) power flow simulators for the evaluation of electrical network configuration changes (that can be both deliberate changes or results from of the effects of accidents and/or attacks) and contingency analysis, (2) real time simulators for the design of protection devices and new controllers. For the telecommunication domain one mat resort to network traffic simulators as for example ns2/ns3 codes that allow the simulation of telecommunication networks (wired/wireless) at packet switching level and evaluate its performances. Single domains simulators can be federated to analyse the interactions among different domains. In contrast, phenomenological simulators use more abstract data and models for the interaction among the different components of the system. The chapter will describe the main characteristic of some of the main simulation approaches resulting from the ENEA and UBC efforts in the CIP and Complexity Science field.

A. Tofani (✉) · G. D'Agostino
ENEA—Italian National Agency for New Technologies,
Energy and Sustainable Economic Development (Italy), Rome, Italy
e-mail: alberto.tofani@enea.it

J. Martí
Department of Electrical and Computer Engineering, University of British Columbia,
Vancouver, BC, Canada

R. Setola et al. (eds.), *Managing the Complexity of Critical Infrastructures*,
Studies in Systems, Decision and Control 90,
DOI 10.1007/978-3-319-51043-9_5

1 Introduction

Phenomenological Modelling: "*Phenomenological models have been defined in different, though related, ways. A traditional definition takes them to be models that only represent observable properties of their targets and refrain from postulating hidden mechanisms and the like*" [1].

The scope of this chapter is to introduce and discuss phenomenological approaches for Modelling Analysis and Simulation (MA&S) of systems involving Critical Infrastructures (CI's). Phenomenological models provide a means to analyse the organizational phenomena of society considering its global complexity (finance, mobility, health, social, energetics, communications, etc.) and the interactions among its different components. With respect to CI's, different modelling approaches have been introduced and used, spanning from very accurate simulators such as "physical simulators" (e.g. power flow simulators for electrical networks) to more abstract ones such as I/O models (e.g. Leontief models for finance).

There is no clear-cut definition of "phenomenological models", however they are normally restricted to those modelling activities based on a massive set of "parameters" to be fed by the modeller. The opposite of the phenomenological models being the "ab initio" ones where parameters are limited to a minimum irreducible set. Alternatively one may qualify phenomenological models as those disregarding internal functional details, thus focussing of the effective response.

Regardless of the semantic boundaries, any MA&S activity relies on a "conceptualization" (i.e. a formal, possibly, mathematical representation) of the inspected system. The first step of any scientific approach to a technological system is its "representation". It is worth noting that an "elective" representation does not exist: depending on the commitment, available information, knowledge and computational means, the "most effective" representation (if any) will be different.

The selection of the model and consequently the simulation paradigm depends on commitment and availability of data. Physical (or Domain) simulators are used to predict the behaviour of the physical system (the technological network) under different conditions and hence to take critical decisions or enforce structural improvements. As an example, the electrical engineers use different kinds of simulators during planning and network management activities depending on their different purposes: power flow simulators are adequate for the evaluation of electrical network configuration changes (that can be both deliberate changes of the effects of accidents and/or attacks) and contingency analysis; while real time simulators are required for the design of protection devices and new controllers. Similarly considerations apply to other energy or goods delivering infrastructures, such as gas, fuel, water transport and distribution. Concerning the telecommunications domain, or other non-conservative distribution systems, one may resort to network traffic simulators, as, for instance ns2/ns3, which allow the assessment of the telecommunication network performance for both wired and wireless architectures.

Single domain simulators can be federated to analyse the interactions among different domains, thus leading to specific simulation activities, which are covered

elsewhere in this book. On the other side, phenomenological simulators may use more abstract data and models for the interaction among the different components of the system, thus providing the global response on the system (i.e. system of systems).

Within the phenomenological MA&S activities, we will shortly cover the approaches underlying the most widespread of them:

- Topological Analyses. Topological and qualitative approaches are suitable for the identification of general characteristics and possibly emergent behaviour of technological networks. In general they do not require very detailed data input and their computational effort is limited. As a consequence, these approaches are suitable for the analysis of general properties of very large networks (e.g. internet) an provide large size effects which may be hidden by details.
- Input-Output Models. In systems engineering and in economics input-output models are based on the concept of "blocks" that have a given transfer function which is expressed with a mathematical formula. The blocks are connected in a certain topological arrangement. For a given block, the output of the block depend on the input to the block. These models can be deterministic when the laws that govern the blocks are well known (e.g., Newton's law) and the blocks will always give the same output for the same input. When the laws that describe the system blocks are not exactly known (or depend on some stochastic factors), the models can be probabilistic (including those that follow stochastic laws), in which case there is only a certain expectation of getting some output for a given input. Among this group it is worth mentioning the Inoperability I/O Model (IIM) [2, 3] and Dynamic IIM models [4].
- System Dynamics. Input-output models provide the output given the input. Mathematically, there are two possible states of a system, the steady state and the transient state. The steady state occurs after the system output settles down for an input that has settled down. However, if the input changes, the output will adapt (if stable) to the new input. The trajectory of the system when transitioning from the initial state to the new state depends on the internal dynamics of the system ("inertia" in physics). The system blocks can be connected to provide each other with positive or negative feedback loops (control systems theory). In economics, these models relate production and consumption variables at a macroscopic level.
- Stochastic Models. In principle all models may be extended to introduce non-deterministic behaviour. In this respect, one may basically identify two different approaches. On one side, one may perform deterministic simulations with a wide range of random boundary conditions [5]; on the other side, the dynamics of the system may be intrinsically stochastic [6].
- Agents simulation. Agent based-functional modelling paradigms are based on representations of the system by different components, each behaving according to given (deterministic or stochastic) rules depending on its status and a limited

set of features of the components they are related to. Agent-based functional modelling approaches, in particular, use a description of the system based on the observed knowledge of how the system behaves under a set of situations. Agents are given attributes according to their observed behaviour. These attributes play a similar role to the transfer function concept in systems engineering, but are described by "if-then" statements rather than mathematical formulas. Agent-based simulation may represent a useful tool to perform exercises, what if analysis and serious gaming. For instance, agent analysis may allow the optimization of crisis scenarios based on previous expert experience.

- I2SIM combines several of the above methods. It uses agent-based concepts to relate system blocks that cannot be described by mathematical equations, such as the operation of a hospital, and mathematical formulas or logical relationships to describe, for example, the operation of transformer and breaker arrangements in an electrical substation. In economics Leontief's production model relates input resources in a sector with the output of that sector linearized around an operating point. I2Sim extends this concept by allowing nonlinear relationships among input resources and output resource and also by including human factors like tiredness, enthusiasm, and others that are not directly part of the input resources but that alter the effectiveness of the process.

As already mentioned, in general, the choice of a suitable approach depends on the quantity and quality of available data, the scale of analysis and the modelling objective [7, 8]. Different approaches can be integrated in order to build complete platforms and tools for comprehensive CI M&S and analysis. Figure 1 shows a possible architecture for a comprehensive modelling, analysis and simulation approach. This proposed architecture highlights the need to manage a possibly huge quantity of heterogeneous data and the different analysis that can be performed on these data. In particular the figure shows the different phenomenological simulators that will be described in the following sections and their main modelling and analysis scope.

The chapter will describe the main characteristics of some of these simulation approaches, in particular those approaches that have been extensively applied in different research projects at ENEA and UBC.

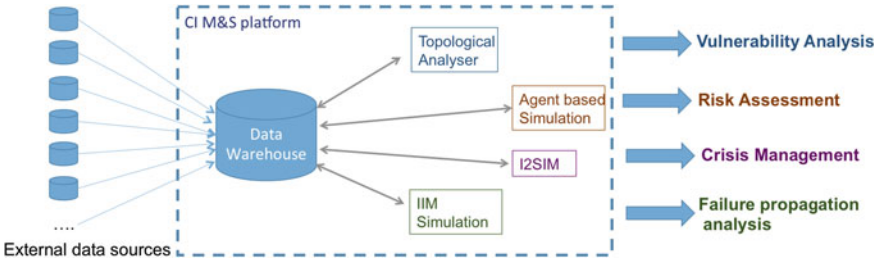


Fig. 1 A comprehensive CI M&S platform architecture

2 Phenomenological Approaches

2.1 Leontief I/O Models

Leontief approaches have been defined mainly for the study of interdependency effects in economic systems. A Leontief model is an Input-Output model where the dependencies among different domains (in the original model, economic sectors) are represented through an input-output matrix to relate the amount of input resources needed for a given amount of finished product. The original Leontief model assumes a linear (or linearized around an operating point) relationship between the input and the output variables.

$$x = Ax + c \Leftrightarrow x_i = \sum_j a_{ij} x_j + c_i \ \forall i$$

The term x_i represents the total output of industry or economic sector *i*, the coefficient a_{ij} represents the dependency between sectors i and j (sector j requires from sector i an amount of resources represented by the coefficient a_{ij}). The term c_i represents the "surplus" from sector i, that is, the output from sector i that is not needed by the other sectors and, therefore, is available as external output from the production system. In the context of CI MA&S the Leontief approach has been extended considering the inoperability of a CI network. The inoperability represents the expected percentage of a network malfunctioning status. I/O models based on inoperabilities are commonly referred to as "Interdependence Input/Output Models (IIM)" and are described in another chapter of this book. The IIM models can be described using the following system of linear equations proposed in [2]:

$$Q_i = \sum_{j=1,..,N} M_{ij} Q_j + \gamma_{iA} D_A$$

where the Q's are components' inoperabilities, M is the relational matrix, D_A is the disturbance and γ_{iA} measures the impact of disturbance on sector j (see also Sect. 2.1.1). Using this approach it is possible to calculate the inoperabilities of a system due to any external disturbance D_A. Beyond its simplicity this model can be useful to understand non trivial systems behavior due to the intrinsic complexity of the system of systems formed by (inter-)dependent CI networks.

In the next section a particular extension adopted in ENEA of the IIM modeling approach is described.

2.1.1 ENEA Extended Leontief Models

As an enhancement of the IIM approach, a Stochastic Chain evolution law may replace the Leontief deterministic one, thus creating a more appropriate tool to

dynamically follow the (stochastic) transition from an equilibrium state to a new one and possibly mimic the cascading effects triggered by unwilled disturbances. Moreover, as a variation of the "System of Systems" approach, each network has not been treated like an holomorphic entity, but its inner structure has been dealt with. Multiple implementations of the same scenarios at different level of granularity have been compared providing evidence for intrinsic inconsistency of high level abstraction models disregarding the actual geographic distribution of network [CRITIS2009].

Indeed, on can extend the former approach to introduce temporal dynamics in the model:

$$Q_i(t+\Delta t) = \sum_{j=1,..,N} M_{ij} Q_J(t) + \gamma_{iA}(t) D_A(t)$$

Considering $\Delta_t \to 0$ the previous equation becomes a stochastic differential equation

$$dQ_i = \sum_{j=1,...,N} h_{ij} Q_J(t)dt + \gamma_i(t) dD_A(t)$$

$dD_A(t)$ represents the "power" of disturbance (disturbance per unit time) and the matrix h is defined as follows

$$h_{ij} = \lim_{\Delta t \to 0} (M_{ij} - I)/\Delta t$$

Considering the constraints that external disturbance and the response of the components are constant and the inoperabilities lie within the [0, …, 1] range in [6] an explicit solution has been given to the previous system of equations. Figure 2 shows a typical evolution of inoperabilities in a CI networks system of systems. The inoperabilities are due to an undesired event directly impacting only one component in the model (*local disturbance*). As it can be seen, the fault propagates affecting other components. After a while the most impacted component is not the one initially perturbed (box in Fig. 2) as may be expected.

Indeed, the systemic behaviour reflect precisely in the fact that response of the system does not dependent on local quantities but on its global characteristics.

2.2 System Dynamics

System Dynamics tries to represent the nonlinear behaviour of a complex system using dynamic stock and flows diagrams. These diagrams are formed by: stocks representing the entities in the model accumulating or depleting over time and by flows representing accumulation rates for the related stocks. System dynamics models include positive and negative feedback loops to relate production and

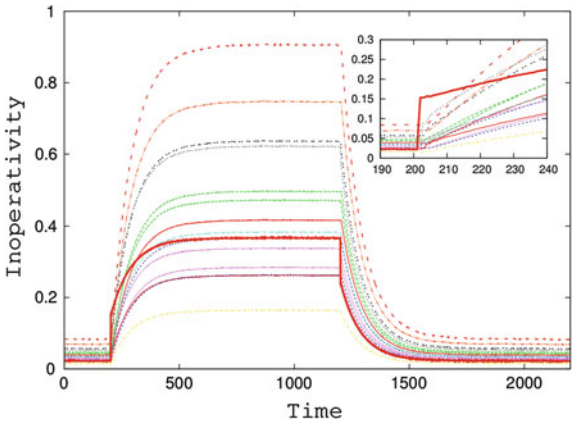


Fig. 2 A example the typical evolution of inoperabilities upon an undesired event impacting on the onset on one component only (*red line*)

consumption variables at a macroscopic level and feedback loops. One of the famous application of System Dynamics model is the Forrester World Model used to predict that the limits to growth of the planet. The Forrester World Model is a flat model (all processes occur in the same layer) that considers the following systems: food, industrial, population, non-renewable resources, and pollution. Considering the CIP field there are a number of approaches that use System Dynamics (SD in the following). For instance, in [9] the SD approach is used to assess the impact of cyber-attacks on critical infrastructures. The methodology compares the behavior of a complex physical process considering two possible situations: the critical assets in its normal behavior and the critical assets under cyber-attack. In this way, the methodology can be used to assess the significance of the considered cyber asset.

The SD approach has been used also in the framework of the CRISADMIN (CRitical Infrastructure Simulation of ADvanced Models on Interconnected Networks resilience) EU project [10] that aims to develop a tool to evaluate the impact of large catastrophic events and/or terrorist attacks on critical infrastructures. The tool is a DSS useful for the assessment and management of critical events. The DSS objective is to simulate preventive measures and emergency responders' activities during an emergency. The DSS is available in the form of a prototype and it was used in four test cases: United Kingdom Flood (2007), Central Eastern Europe Flood (2002), Madrid terrorist attack (2004), and London terrorist attack (2005).

2.3 i2SIM

The I2Sim (Integrated Interdependencies Simulator) was developed at The University of British Columbia to extend the capabilities of large engineering systems simulation by incorporating phenomena that cannot be expressed in terms of mathematical transfer functions [11]. For example, the operation of a hospital in terms of patients accepted per hour cannot be capture by physical equations, but it is

management	engineering	engineering	management	management	engineering	management
y(t)	**$x_1(t)$**	**$x_2(t)$**	**$m_1(t)$**	**$m_2(t)$**	**$m_3(t)$**	**$m_4(t)$**
Patients per hour	**Electricity (kW)**	**Water (L/h)**	**Doctors**	**Nurses**	**Physical Integrity**	**Doctors Shift Factor**
20	100	2,000	4	8	100%	100%
15	75	1,00	3	6	80%	75%
10	50	600	2	4	50%	50%
7	25	400	2	3	20%	25%
0	0	0	0	0	0%	0%

Fig. 3 HRT for a hospital emergency unit

known to the hospital manager and can be captured in an input-output table that is called an HRT (human readable table).

Figure 3 shows an example of an HRT for a hospital emergency unit.

In the table, the full operation of the hospital, 20 patients per hour, is achieved when the electricity is 100 kW, the water is 2000 l/h, there are 4 doctors and 8 nurses, there is no physical damage (for example, due to an earthquake) and the doctors are not tired. In the scenario (circled values), there is no lack of electricity or doctors, but there are limited resources in terms of nurses, physical integrity, some tiredness of the doctors, and mostly lack of water. The output in this example is limited to 10 patients per hour due to the lack of enough water.

Figure 4 shows a simple sample system for i2Sim. The production units in i2Sim are called "cells" (Fig. 5a) that receive inputs (physical or modifiers) and produce

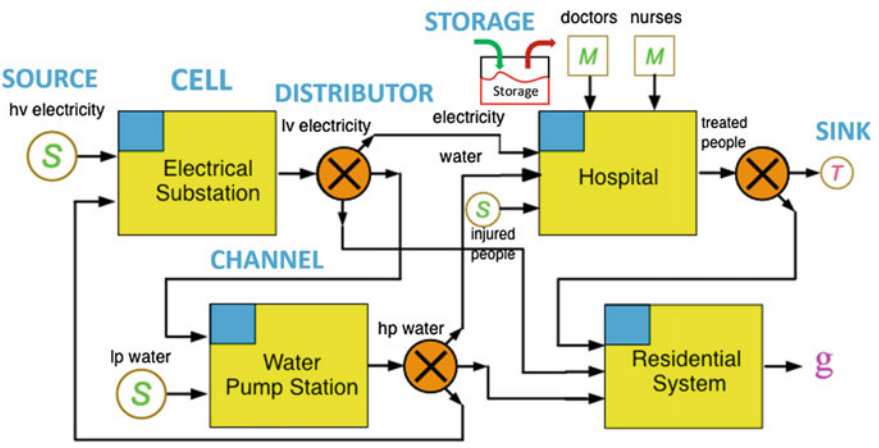


Fig. 4 i2Sim ontology illustrated in simple system

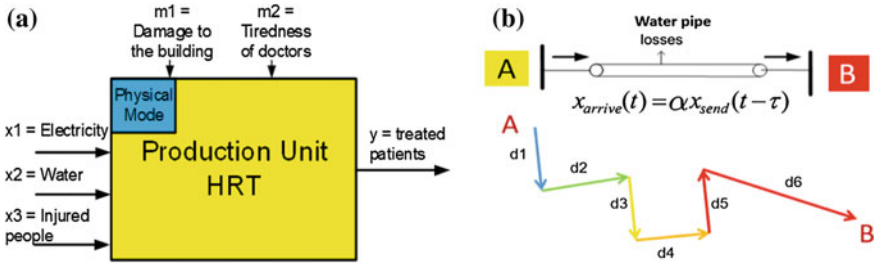


Fig. 5 An I2Sim cell (**a**) and channel (**b**)

one output. Other basic ontological elements include the connection among cells "channels" (Fig. 5b) that deliver the tokens from one cell to another (Fig. 5b). Channels may introduce losses and delays in the delivery of the tokens. The channels constitute an equivalent of the token transportation system. For example, there are many pieces of water pipes connecting the water pump station and the hospital, but a single equivalent channel can capture the water losses due to cracks in the pipes. At the output of the cell, there is a "distributor" that splits the output of the cell into the portions (ratios) delivered to the other cells. How the split ratios are determined is a "decision" made in a separate layer outside the system in the figure. The split of the outputs at the distributors is fundamental to optimize the total system objective, e.g. save lives during a disaster.

The fundamental problem during a natural disaster, cyber-attack, or system failure, is that the resources that the system uses during normal operation will be limited because of the damage caused by the event. The decisions at the distributors are made by optimizers, either of mathematical or human type. Figure 6 shows the HRT for an electrical system substation that normally delivers 60 MW of electricity. If one of the two transformers is damaged then the output will be limited to 30 MW and a decision will have to be made as to which customers will receive the

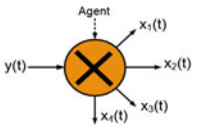
Fig. 6 HRT model for an electrical system substation

HRT For Electrical Substation

Output y(t)	Source $s_1(t)$	Condition $m_1(t)$
Low Voltage Power (MW)	High Voltage Power (MW)	Transformers Working
60	60	2
30	30	1
0	0	0

Distributor

Agent Decision: Choose 2 out of 4 feeders



available power. This decision should be made in terms of the importance of the cells that will receive this power within the global objective function of the system. For example, during a disaster the global objective will be to save human lives. It then makes sense to send all the available power to the hospitals. However, if the water pump stations do not receive power, the hospital will not be able to operate, not because of the lack of electricity but because of the lack of water. The allocation of the available electricity, water, and other resources is a mathematical optimization problem that changes dynamically in time as system repairs are made and further damage occurs. The i2Sim framework allows the incorporation of physical, cyber-physical, organizational, and human variables within the context of optimizing the global system's objective.

I2Sim follows a layered approach (Fig. 7) at integrating physical and non-physical phenomena. The layers illustrated in Fig. 7 include: the Physical Production Layer (similar to Leontief's production layer, expanded to include nonlinear relationships and human factors), the Geographical Damage Layer (that will include the calculations of the damage caused by and earthquake, for example), the Management and Organizational Layer (that will include the policies and procedures that regulate who makes what decisions), the Cyber-system Layer (that includes the signals that control the actions to actuate the physical equipment and the communications among managers and responders), and the People's Well-being Layer (that includes, for example, the results of the actions of the system in terms of consequences on quality of life).

I2Sim's solution engine has the capability of handling very large systems so that the degree of detail in the sub-systems and their interactions is limited mostly by the degree of resolution of the data available and the uncertainty of the values of these data.

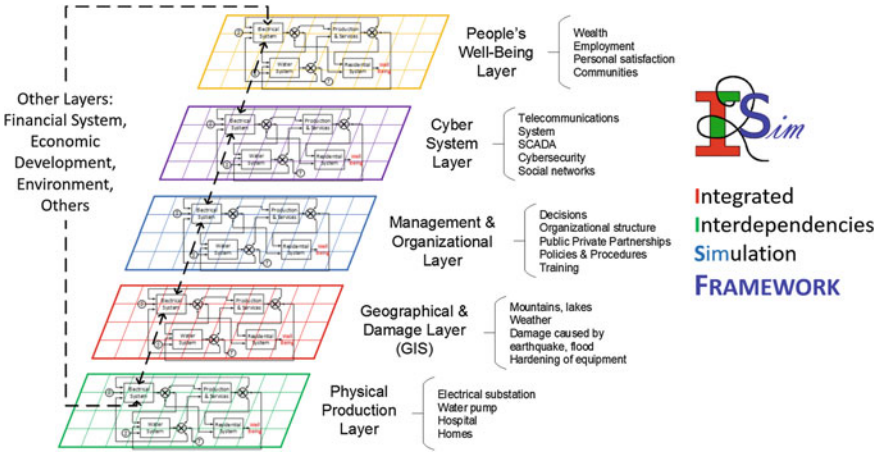


Fig. 7 i2Sim multi-layered framework

Structurally, i2Sim follows the Multi-Area Thévenin Equivalent (MATE) concept developed for the simulation of large power systems [12]. The main predicate of MATE is that a large system is made up of smaller subsystems with links among them. Algorithmically, the MATE solution proceeds in several parallel/sequential stages: first the subsystems (of lower dimensionality than the full system) are solved separately (possibly eventually simultaneously in parallel processors). Then the dimensionality of each subsystems is reduced down to equal the number of links that connect the particular subsystem to the other subsystems (Thévenin equivalents). Then the Thévenin equivalents are brought together to form the links-subsystem of dimensionality equal to the total number of links. The links subsystem is now solved. The solution will give the flow in and out of the links connecting the subsystems. Finally, the individual subsystems are "updated" with the links solution. This concept has been generalized in i2Sim for the general framework of Fig. 7.

In the sample system of Fig. 4, the source resources are provided by utilities that may constitute a complete infrastructure subsystem, for example, the electrical grid, the water system, the transportation system, the telecommunications system, and others. Similarly, the outputs of some of the i2Sim cells can be given out to other infrastructures in an action that is opposite to that of a source, that is, into a load/sink. Each one of these subsystems can be modelled with a separate simulator (Fig. 8) which is best suited to the scenario under analysis. These "federation of external simulators" is coupled to the i2Sim "links subsystem". The links subsystem is then optimized according to a global objective function in a process that involves the updating of the external subsystem, as described for MATE.

The federated simulators in Fig. 8 are coupled together through software adapters into a common service bus. The simulation proceeds along the time line using a master clock controller (Fig. 9).

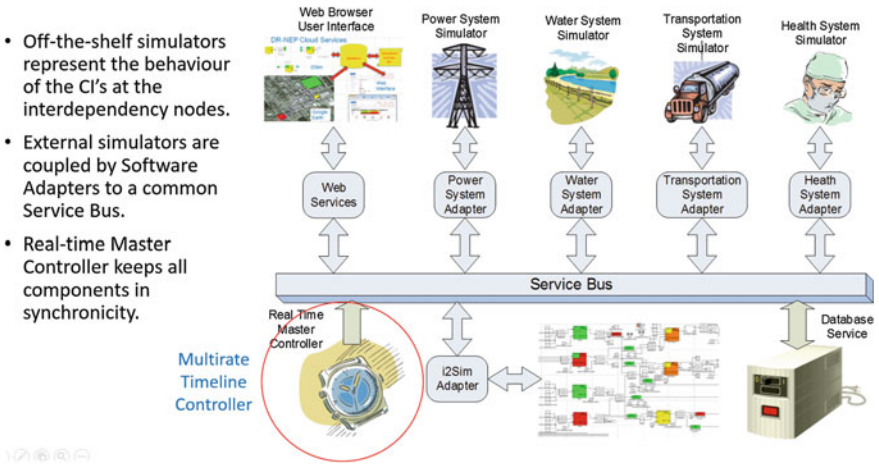


Fig. 8 Federated source/load simulators

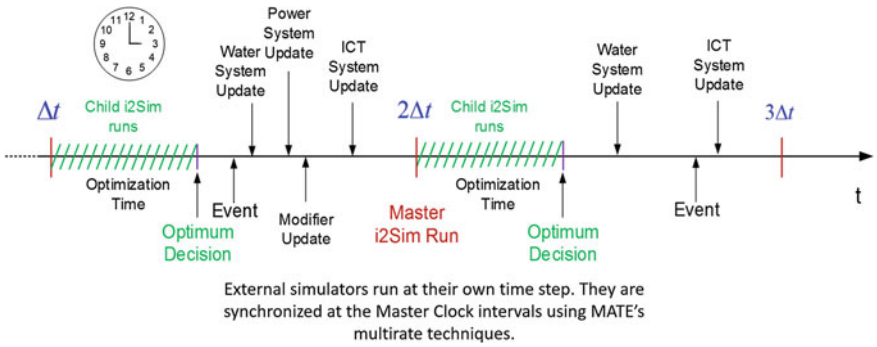


Fig. 9 Multirate time controller

The federated simulators in Fig. 8 are coupled together through software adapters into a common service bus. The simulation proceeds along the time line using a master clock controller (Fig. 9). The different subsystems that constitute the integrated i2Sim framework will have different response times (different "time constants"). For example, the supply of electricity can be controlled within seconds or milliseconds, while the water system may take a few minutes, and the organizational system of a hospital or emergency response management unit may take longer. To coordinate these different response rates, i2Sim uses multirate concepts developed in signal processing and simulation theory. The MATE solution framework allows for the integration of multirate concepts using interpolation and decimation techniques to maintain the synchronicity of the solution.

In addition to the optimization of resources allocation during disasters management, i2Sim can also be applied to evaluate the resiliency of a city or a region. In the case, for example, of a "smart city", the recovery of the system of infrastructures after a natural disaster, cyber attack, or equipment failure should be managed in such a way that the most critical services are restored first. The overall objective in this application is to maximize the well-being of the citizens and this well-being can be mapped into a resilience index [13].

Figure 10 illustrates an example of a city where some basic infrastructures, electricity, water, and ICT have suffered damage and their delivered resources are limited. In this case the system objective function is to maintain the well-being of the city residents. We define a Well-Being Index (WBI) ("wee-bi") using an HRT that shows the relative importance of the availability of certain services, in this example, electricity, water, general city services (banking, food, etc.), and ICT (internet, etc.). This is a subjective index that will depend on the area of the city and the country and will require the collaboration of social scientists and psychologists to define. The global objective of the optimization problem is to maximize the resiliency index based on this HRT table. Notice that the WBI can be highly nonlinear. This example further illustrates the capability of i2Sim to incorporate human factors into the system solution.

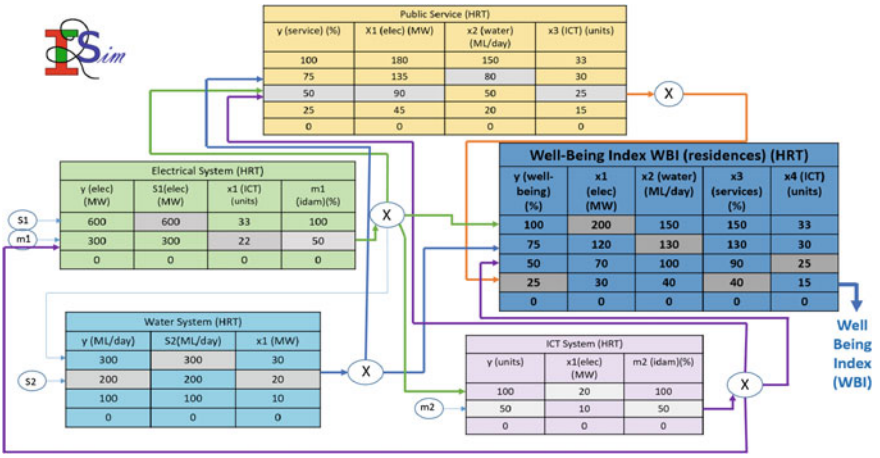


Fig. 10 City resiliency and well-being index (WBI)

The HRT tables in i2Sim provide the flexibility to incorporate physical and non-physical factors into the same solution framework. In addition, since these tables may have a limited number of rows, the detail in the description can be adapted to the amount/uncertainty of knowledge for a given cell entity. The simplest HRT would have two rows indicating that the cell is either operating at full capacity (100%), or is totally non-operative (0%). In a more detailed analysis, with higher granularity of information, the number of rows would be larger. The tables in Fig. 10 have different granularities. The combinatorial solution of i2Sim uses the discrete HRT tables to find the optimum combination of rows across all cells in the system that maximizes the output objective function over a certain time scenario. Two optimization methods that have been successfully applied include reinforcement learning [14] and ordinal optimization [7].

In very large systems, however, with a large number of cells, distributors, and other components, a combinational solution can have very high dimensionality. An alternative solution to this problem is to convert the discrete relationships in the HRTs into continuous analytical functions. Figure 11 illustrates the analytical-i2Sim

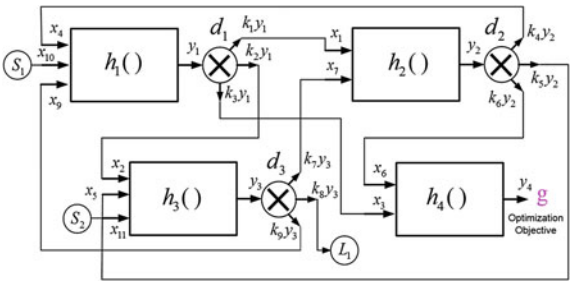


Fig. 11 Analytical-i2Sim solution

version. In this version, the columns of the HRTs are synthesized using continuous hyperbolic function approximations.

With the HRTs represented by functions *h(t)*, a system of equations can be formed where each cell contributes an equation of the form

$$y_i = \min\{q_1(x_1), q_2(x_2), q_3(x_3)\}$$

where q_i is the function that approximates column i in the HRT. The q_j functions are assumed to be linearly independent. The cell equations can now be combined with the distributor equations, and the equations for the other components in the i2Sim ontology, to form a system of nonlinear equations that can be solved using a Newton-Raphson algorithm. The trajectory of the system towards maxima and minima can be tracked using the associated Hessian matrix for gradient-type methods of optimization. This work is currently under development. A variation of this analytical method, that involves a first-order approximation of the q_j functions combined with a linear programming algorithm, has also been developed. This version can achieve orders of magnitude faster solutions and can be used as a good first-order approximation to many problems or as a starting base-point for systems with stronger nonlinearities. The optimization along a time line of the event can be obtained using machine learning techniques such as reinforcement learning [14].

3 Topological Analysis

Electrical power transmission and distribution networks, telecommunication (data, voice) networks, roads, oil and gas pipelines etc. are objects that can be easily represented as graphs where nodes represent different CIs components and the links represent their connections (e.g. logical, physical). In this respect there is a large deal of efforts in applying ideas and methods of Complex Systems (CS) to them, particularly to study their vulnerability and their response to fault. The main aim is to increase their resilience and to reduce the effects that a fault, regardless of its accidental or intentional origin, might produce. In the following some basic definitions of the graph theory.

A graph $G = (V, E)$ is composed by a set of nodes V and a set of edges E. An edge $e = (v_i, v_j) \in E$ connects the vertices $v_i, v_j \in V$. A graph may be *undirected*, meaning that there is no distinction between the two vertices associated with each edge, or its edges may be *directed* from one vertex to another. A graph may be *unweighted* or *weighted*. In the latter case each $e \in E$ has associated a real number w_e. The *degree* of a node is the number of links entering (and/or leaving) from it. A graph can be fully represented by an Adjacency matrix A. For example, the Fig. 12 shows a graph example and its adjacency matrix.

The simplest indicator of how intensely a node is connected to the rest of the net is its ***degree*** defined as the number of nodes it is connected to or, equivalently, the total number of incoming and outgoing links entering or exiting from it:

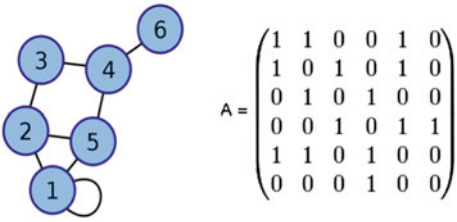


Fig. 12 A graph example and its related adjacency matrix

$$deg_i = \sum_{j=1}^{N} a_{ij}$$

The degree distribution P(k) is introduced defined as the (relative or absolute) frequency of nodes of degree k. According to this property a graph can be classified as regular, random or scale free. Figure 13 shows the difference between the node degree distribution of random and scale-free graphs. In Fig. 14 two examples of graphs are depicted (Fig. 15).

The functional form of P(k) contains relevant information on the nature of the network under study. It has widely shown that "real" spontaneously-grown networks (i.e. grown with no external design or supervision) tend to show a power-law decaying P(k). In this type of networks (named "scale-free" networks), loosely connected nodes (*leaves*) and highly connected ones (*hubs*) co-exist. Scale-free networks are known to exhibit a high level of robustness against random faults of their elements, while showing a large vulnerability related to the removal of specific components: *hub* removals induce dramatic impacts on the graph connectivity. "Random" graphs, in turn, are those whose P(k) has a poissonian profile. The "random graph" approximation, although being used to map most of "real" networks, has been discovered to represent very few real systems [15].

Different statistical indices may be introduced to describe the degree distribution. For instance it is possible to compute the range of the node degrees using the

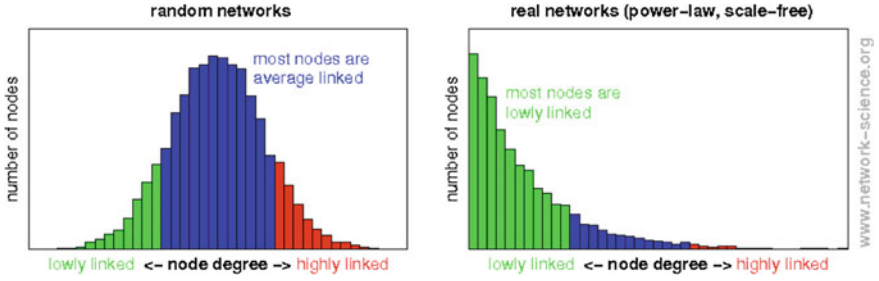


Fig. 13 Random and scale free node degree distribution

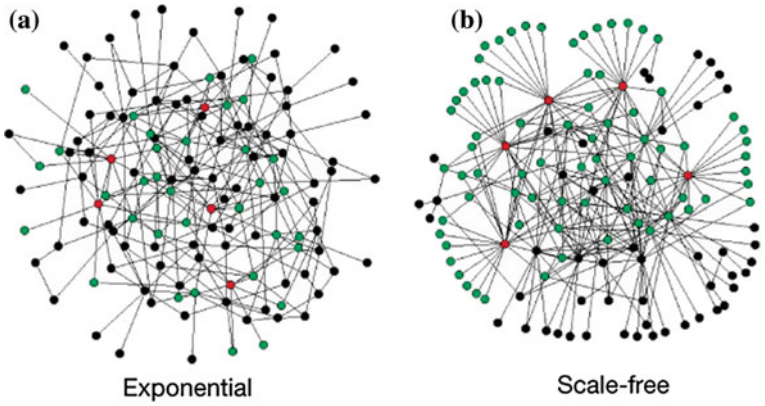


Fig. 14 Example of random (or exponential) and scalar-free graphs [21]

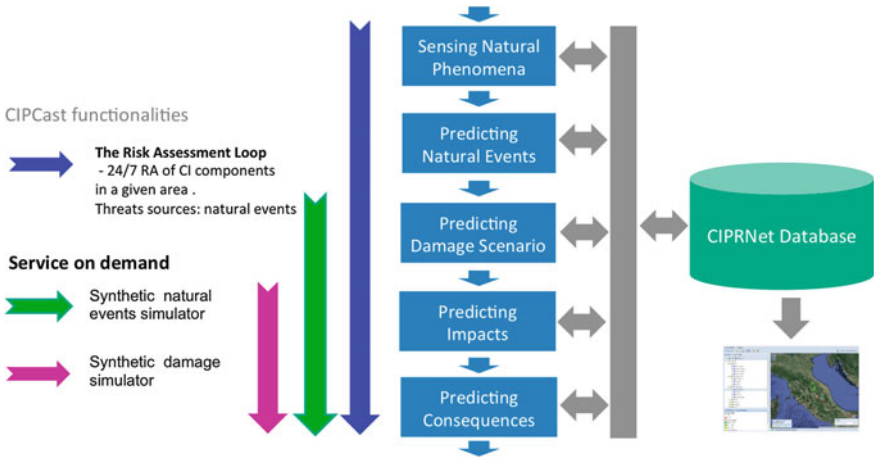


Fig. 15 The CIPCast workflow

minimum and maximum degree in the network. Then we have the average degree and variance defined as follows:

$$\langle deg \rangle = \frac{1}{N} \sum_{s=1}^{N} deg_s$$

$$\sigma_{deg}^2 = \frac{1}{N-1} \sum_{s=1}^{N} \left(deg_s^2 - \langle deg \rangle \right)^2$$

To better describe the topological structure of a network it is possible to introduce the conditional degree distribution that is the probability that of a node of degree k_0 has a neighbor of degree k:

$$P(k|k_0) = \frac{\sum_{(i,j)\in E} a_{ij}\delta_{deg_i,k}\delta_{deg_j,k_0}}{\sum_{(i,j)\in E} a_{ij}\delta_{deg_j,k_0}}$$

The last coefficient that will be reported in this work is related to the degree correlation. In particular when nodes of high correlation tend to be linked to nodes of high correlation, the net is said to be *assortative*, vice versa when high degree nodes tend to be linked to low degree ones the net is said to be *disassortative*. This coefficient can be defined as follow:

$$r = \frac{\frac{1}{L}\sum_{ij} a_{ij} deg_i deg_j - \left(\frac{1}{L}\sum_{ij} a_{ij}\frac{1}{2}(deg_i + deg_j)\right)^2}{\frac{1}{L}\sum_{ij} a_{ij}\frac{1}{2}\left(deg_i^2 + deg_j^2\right) - \left(\frac{1}{L}\sum_{ij} a_{ij}\frac{1}{2}(deg_i + deg_j)\right)^2}$$

In [16] the authors analyzing the diffusive dynamics of epidemics and of distress in complex networks shows that disassortative networks exhibit a higher epidemiological threshold and are therefore easier to immunize, while in assortative networks there is a longer time for intervention before epidemic/failure spreads. Then, the robustness of complex networks is related to the its assortative coefficient.

Using definition coming from the graph theory and different topological indices, several possible analysis are performable on a CI network. The MOTIA project [15] used the topological approach to study the main characteristics of ICT networks consisting of a set of devices or components (server, bridges etc.) connected by cables or wireless channels (links). The next table summarizes the possible properties that can be analyzed using the topological analysis approach [MOTIA].

Given a graph representation of an ICT network it is possible to calculate the topological indices reported in Table 1 to analysis the network characteristics. One of the most important property to consider is represented by the *network robustness*. The *robustness* indicates to what extent net topological properties are stable against damages. For example, there are two basic concepts of connectivity for a graph, which can be used to model network robustness: *node-robustness* and *link-robustness*. The "node robustness" of a net is the smallest number of nodes whose removal results in a disconnected or a single-node graph. Conversely, the "link robustness" is the smallest number of links whose removal results in a disconnected graph [17]. In [15] the authors uses the described topological indices to analysis the internet network.

Table 1 Topological indices

Connectivity	A graph is connected if all nodes are connected (or reachable) each other	
Distance	The distance d(i, j) between two vertices (i and j) belonging to a connected part of a graph is the length of one of the shortest paths between them. The distance is symmetric (d(i, j = d(j, i)) only when the net is undirected	
Eccentricity	The eccentricity ε(i) of a node i in a connected graph G is the maximum of the distances from i to any other node	
Diameter	The diameter diam (G) of a connected part G of graph is the maximum eccentricity over all its nodes	
Radius	The radius rad(G) represents the minimum of such eccentricities	
Wiener index of a node	The Wiener index of a node i, denoted by W(v) is the sum of distances between it and all the others	$C_W(i) = \sum_{j \in N} d(i,j)$
Wiener index of a graph	The wiener index of a graph G, denoted by W(G), is the sum of distances over all pairs of vertices	$C_w = \sum_{i=1}^{N} C_w(i) = \sum_{i,j=1}^{N} d(i,j)$
Centrality	Relevance of a node to provide some type of property to the others	
Betweenness	For a node i this index represents the sum of the fractions of paths connecting all pairs passing throw it. The number of paths connecting two different nodes j and k, will be indicated by n^{jk} while the number of such paths passing through the node i will be indicated by n_i^{jk}	$b_i = \sum_{j,k=1}^{N} \frac{n_i^{jk}}{n^{jk}}$
Clustering	The clustering coefficient c provides a parameter to measure the connectivity inside the neighborhood of a give node. In general, nodes of low clustering values might represent region of weakness on the network	$C_i = \frac{2N_i^{links}}{deg_i(deg_i - 1)}$ N_i^{links} represents the number of links among the neighbors of the i-th site

4 A CI MA&S Platform for Complex and Large Scenarios

This chapter describes the approaches used in the framework of the EU-FP7 CIPRNet project http://www.ciprnet.eu. One of the main technological outcomes of the CIPRNet project is a DSS, named CIPCast that is able to provide a 24/7 service to CI operators and emergency (crisis) decision-makers providing a continuous risk assessment of CI elements due to natural threats. CIPCast has been designed and

implemented to allow the prediction and rapid assessment of the consequences of a crisis scenario in an "operational" mode of operation (24/7). CIPCast, however, can also be used in an "off-line" mode for producing risk analysis starting from synthetically produced events (rather than truly occurring ones) or from synthetically produced damages (rather than by damages produced by true or synthetic events). In the former case, we will talk of "event simulator", in the latter of "damage simulator". One of the main components of CIPCast (when acting in the "operational" mode) is a continuous process (running on a 24/7 basis) realizing the Risk Assessment Loop, RAL in the following (as shown in Fig. 15). Starting from the prediction of the occurrence of natural hazards and of their strengths, RAL first estimates the expected damages, then transforms the damages into effects that they will produce on all Services (carried out by CI) which will be reduced (or switched off) and, subsequently, estimating the consequences that the loss (or reduction) of Services would have on relevant areas of societal life. The tool can also be used to "weigh" the efficacy of the proposed mitigation and healing actions and thus being a valuable tool for supporting emergency managers e.g., CI operators, Civil Protection and fire brigades.

This section describes a specific RAL workflow instance that has been implemented for the natural hazard risk assessment of electrical distribution networks. In particular, the described workflow is related to the heavy rain risk assessment of the electrical distribution network of Rome. The workflow has been implemented in cooperation with the Italian RoMA project partner ACEA that is the main electrical utility in Rome. Specifically, the section will show how the different phenomenological simulators for CIs can be used as the building bricks of different phases of the workflow and in general, for the realization of additional services for the DSS end users.

The first challenge to face during the development of such kind of platforms is the acquisition of CI networks data. In order to perform a comprehensive risk analysis these data need to be related to the different aspects involved in the management of the CI networks. Indeed, the basic requirement to build comprehensive models and, successively, comprehensive simulation and analysis is to dispose of data related to CI networks physical components and network management procedures (considering the differences between the procedures adopted in normal state and during a crisis). Then, the next step for any MA&S activity is the "conceptualization" of the inspected systems and to build formal representations. In [18] the authors propose UML extensions (meta-models) in order to define the different aspects of an infrastructure organization and behaviour as ownership and management, structure and organization, resources, risk and relationship. The CEML language proposed in [19] is a graphical modelling language allowing domain experts to build formally grounded models related to crisis and emergency scenarios. In general the infrastructure scale of analysis describes the level of granularity the infrastructure interdependencies are analysed and which kind of approaches can be used in the analysis. At a high abstraction level the interdependent networks can be modelled and analysed from the system of systems point of view. At this level of granularity it is possible to build graph models or the IIM. In the former case, the topological

approach can be applied to compute the different coefficients, indices described in Table 1 to assess for example the robustness of the networks or possible components vulnerabilities. In the later case IIM models can be used to perform failure propagation analysis. Then, going to a lower abstraction level and thus requiring more detailed data, it is possible to use agent-based approaches or I2SIM to perform networks and crisis scenario analysis considering functional properties of network components, network management procedures and phenomenological factors that cannot be represented by more abstract models (see Fig. 17). In particular, CIPCast includes the RECSim simulator [20] (as shown in Fig. 16) that allows the simulation of the electrical distribution network management procedures and its interdependencies with the telecommunication domain. Indeed, electrical distribution operators use SCADA systems to perform remote operations (tele-control) on the electrical grid to ensure a constant and efficient energy supply to the consumers. Tele-control operations bi-directionally couple telecommunication and electrical networks: faults in one network produce effects, which in turn reverberate on the others. RECSim assesses the correct tele-control operations needed for the restoring of the electrical grid based on topological properties of the electrical substations and the Telecom nodes. A crucial approximation introduced in CIPCast is the decoupling of the electrical and telecom systems form all the other infrastructures. These networks should be considered highly dependent and tightly linked; for this reason, their behaviour and their mutual perturbation dynamics occur in times, which are much shorter than those characterizing the perturbation dynamics for other infrastructures. As such, electro-telecom dynamics are resolved at first, in a time scale typical of their interaction (from a few seconds to a few hours) by keeping the other infrastructures substantially unperturbed. Once the electro-telecom perturbation dynamics has been

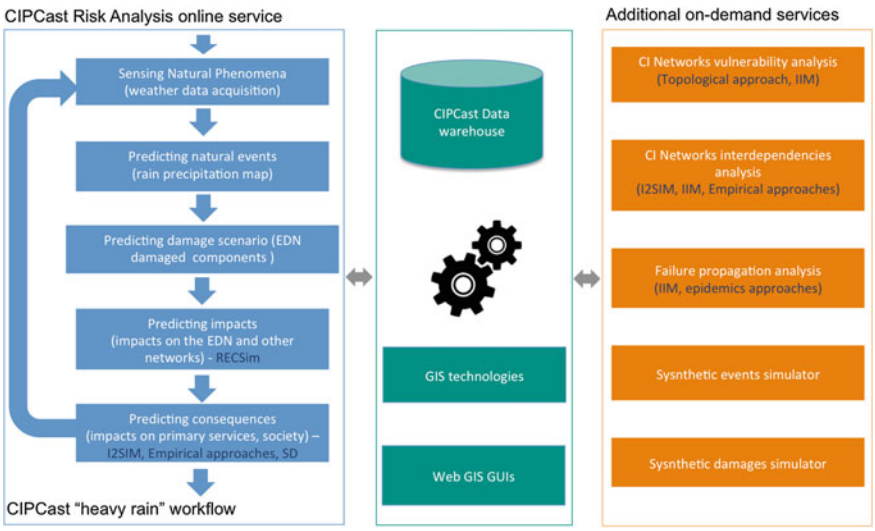


Fig. 16 The CIPCast risk analysis service workflow

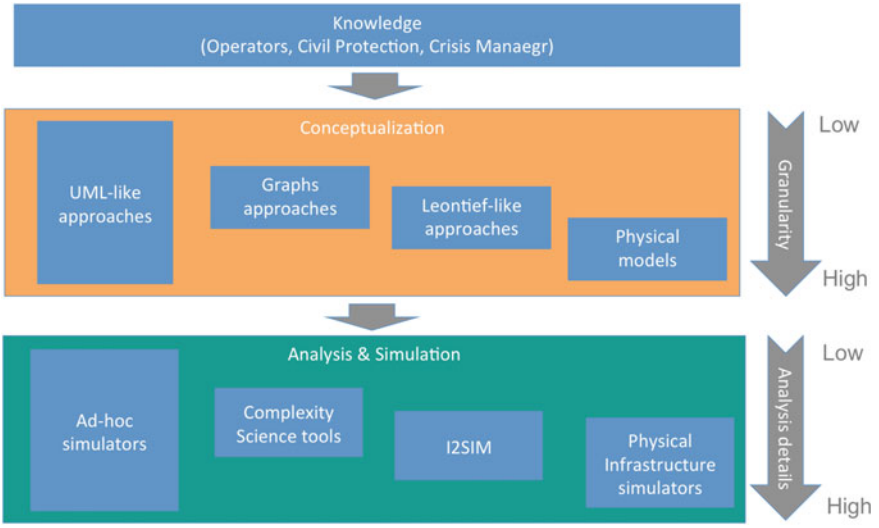


Fig. 17 From knowledge to simulation

solved, the resulting electro-telecom situation (inoperability) is introduced in the complete infrastructures setting in order to estimate the further perturbation produced on the other infrastructures (using I2SIM).

5 Conclusion

The document describes the results of several years of research at ENEA and UBC in the field of Critical Infrastructure Protection and *Complexity Science*. In particular, the document describes some phenomenological simulators for complex systems of CI's and highlights how these tools can be considered as fundamental pillars of a CI MS&A platform. This framework allows various kind of analyses for different end users and, in general, for different objectives. Regardless of the analysis objective, the first step is to build a valid and effective representation of the inspected system. It is worth noting once again that an "elective" representation does not exist: depending on the commitment, available information, knowledge and computational means, the "most effective" representation (if any) will be different. Therefore, different phenomenological approaches are currently applied. The paper proposes a general framework and platform architectures to integrate the main components of any CI MA&S approach. It further shows the details of the CIPCast and the I2sim platforms that are compliant with the proposed general paradigm. The CIPCast platform, developed within the CIPRnet project, is a Decision Support System providing a 24/7 service to CI operators and emergency (crisis) decision-makers providing a continuous risk assessment of CI elements due to natural threats. One of the main components of CIPCast (when acting in the

"operational" mode) is a continuous process (running on a 24/7 basis) realizing the Risk Assessment Loop (RAL). Within the RAL, an agent based simulator (RECSim) developed by ENEA and the I2SIM simulator have been used allowing the simulation of the electrical distribution network management procedures (considering the interdependencies between the electrical and the telecommunication domain) and, once the resulting electro-telecom situation (inoperability) has been assessed, the further perturbation produced on the other infrastructures is assessed using I2SIM. In the future, as more technological infrastructures data will be available for a specific area, CIPCast will be enriched using complete system of systems representation of the (inter)-dependent networks. Thereby, all other approaches described in the document, as for example topological ones and IIM models, will be available in real time to perform different analysis as failure propagation and vulnerability analysis. CIPCast can be used to discover intrinsic vulnerabilities of the technological networks (i.e. vulnerabilities that depend on how components are connected to others of the same or different infrastructures). Ultimately, CIPCast will result in a comprehensive decision support system also allowing for investments planning to improve resilience and mitigate the risk.

Acknowledgement and Disclaimer This chapter was derived from the FP7 project CIPRNet, which has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 312450.

The contents of this chapter do not necessarily reflect the official opinion of the European Union. Responsibility for the information and views expressed herein lies entirely with the author(s).

References

1. Frigg R, Hartmann S (2012) Models in science. In: Zalta EN (ed) The stanford encyclopedia of philosophy (2012 edition). URL: http://plato.stanford.edu/archives/fall2012/entries/models-science/
2. Haimes YY, Jiang P (2001) Leontief-based model of risk in complex interconnected infrastructures. J Infrastruct Syst 7(1):1–12
3. Santos JR, Haimes YY (2004) Modeling the demand reduction input-output (I-O) inoperability due to terrorism of interconnected infrastructures. Risk Anal 24(6):1437–1451
4. Lian C, Haimes YY (2006) Managing the risk of terrorism to interdependent infrastructure systems through the dynamic inoperability input-output model. Syst Eng 9(3):241–258
5. Cavalieri S, Chiacchio F, Manno G, Popov P (2015) Quantitative assessment of distributed networks through hybrid stochastic modeling. In: Bruneo D, Distefano S (eds) Quantitative assessments of distributed systems: methodologies and techniques. Wiley, Hoboken. doi:10.1002/9781119131151.ch9
6. D'Agostino G, Scala A (2015) Systemic interdependences. In: Handbook of science and technology onvergence. Springer International Publishing, Switzerland. doi:10.1007/978-3-319-04033-2_14-1
7. D'Agostino G, Scala A (2014) Networks of networks: the last frontier of complexity. In: Understanding complex systems. Springer, Berlin
8. Satumtira G, Dueñas-Osorio L (2010) Synthesis of modeling and simulation methods on critical infrastructure interdependencies research. In: Sustainable and resilient critical infrastructure systems. Springer, Berlin, pp 1–51

9. Genge B, Kiss I, Haller P (2015) A system dynamics approach for assessing the impact of cyber attacks on critical infrastructures. Int J Crit Infrastruct Prot 10:3–17
10. http://crisadmin.eu
11. Martí JR (2014) Multisystem simulation: analysis of critical infrastructures for disaster response. In: D'Agostino G, Scala A (eds) Networks of networks: the last frontier of complexity. Springer International Publishing, pp 255–277
12. Armstrong M, Martí JR, Linares L, Kundur P (2006) Multilevel MATE for efficient simultaneous solution of control systems and nonlinearities in the OVNI simulator. IEEE Trans Power Syst 21(3):1250–1259
13. Alsubaie A, Alutaibi K, Marti JR (2015) Resilience assessment of interdependent critical infrastructure. In: The 10th international conference on critical information infrastructures security (CRITIS), Berlin, pp 1–12, 5–7 Oct 2015
14. Khouj M, Sarkaria S, Martí JR (2014) Decision assistance agent in real time simulation. Int J Crit Infrastruct Syst 10(2):151–173
15. MOTIA (Modelling Tools for Interdependence Assessment in ICT Systems) Project Report Activity 5 Metrics Definition, 2012
16. D'Agostino G, Scala A, Zlatić V, Caldarelli G (2012) Robustness and assortativity for diffusion-like processes in scale-free networks. Eur Phys Lett 97(6):68006
17. Gill NS, Balkishan (2008) Dependency and interaction oriented complexity metrics of component-based systems. In: ACM SIGSOFT software engineering notes, vol 33, no. 2, Jan 2008
18. Bagheri E, Ghorbani AA (2010) UML-CI: a reference model for profiling critical infrastructure systems. Inf Syst Front 12:115–139
19. De Nicola A, Tofani A, Vicoli G, Villani ML (2011) Modeling collaboration for crisis and emergency management. In: COLLA 2011: the first international conference on advanced collaborative networks, systems and applications
20. Tofani A, Di Pietro A, Lavalle L, Pollino M, Rosato V (2015) CIPRNet decision support system: modelling electrical distribution grid internal dependencies. In: Proceedings on critical infrastructures preparedness: status of data for resilience modelling, simulation and analysis (MS&A), ESReDA workshop, Wroclaw, 28–29 May 2015
21. Albert R, Jeong H, Barabási AL (2000) Error and attack tolerance of complex networks. Nature 406:378–382. doi:10.1038/35019019

Chapter 6
Federated Simulations

Wim Huiskamp and Tom van den Berg

Abstract The integration of simulation components into a federated, interoperable simulation environment introduces a large number of engineering challenges. Many of these challenges are technical issues, but there are also several challenges from the project management perspective. For example, when simulation components are provided by different organizations from different domains there is a need to ensure coordinated and timely interaction among these organizations, and a need for a common view on the engineering process. Recognizing and mitigating these technical and project management issues are critical to controlling risk across a simulation development effort. This chapter provides an overview of several standards that have been developed over time in the area of distributed (or federated) simulation. These standards address both simulation environment architecture and engineering process. This chapter starts with an introduction to distributed simulation, followed by an overview of:

- the High Level Architecture (HLA), a technical standard for distributed simulation environments;
- the Distributed Simulation Engineering and Execution Process (DSEEP), an engineering process to address the needs of a very large and diverse user community in the engineering of distributed simulation environments;
- the Federation Agreements Template (FEAT), a standardized format for recording simulation environment agreements to increase their usability and reuse.

W. Huiskamp (✉) · T. van den Berg
Netherlands Organisation for Applied Scientific Research (TNO),
Oude Waalsdorperweg 63, 2597 AK The Hague, The Netherlands
e-mail: wim.huiskamp@tno.nl

R. Setola et al. (eds.), *Managing the Complexity of Critical Infrastructures*,
Studies in Systems, Decision and Control 90,
DOI 10.1007/978-3-319-51043-9_6

1 Introduction

Critical Infrastructures are complex systems of systems. They are interdependent and if one part fails there may be cascading effects on other parts in the system, sometimes with catastrophic results. Different modeling approaches have been employed to capture their behavior, analyze their interdependencies and vulnerabilities, and forecast the effects on other systems, environment and people. Modelling approaches include agent based modelling, system dynamics modelling, and input-output modelling.

Developing a single simulation model for such a complex system of systems is a hard to impossible task. Large monolithic simulation models are generally hard to re-use and no single simulation model can solve all problems. In some instances simulation models must be federated in order to be able to analyze the system of interest, simply because there are no other options. In addition, smaller simulation models of suitable granularity provide more flexibility and opportunities for model reuse. Therefore it makes sense to federate disparate simulation models of Critical Infrastructure in a single simulation environment. This idea is illustrated in Fig. 1, where three simulation models are connected through some run-time infrastructure.

The integration of simulation models in a federated, interoperable simulation environment introduces several engineering challenges. Many of these challenges are technical issues, but there are also challenges from the project management perspective. For example, when simulation models are provided by different organizations in different domains, there is a need to ensure coordinated and timely interaction among these organizations, and a need for a common view on the engineering process. Recognizing and mitigating these technical and project management issues are critical to controlling risk across a simulation development effort.

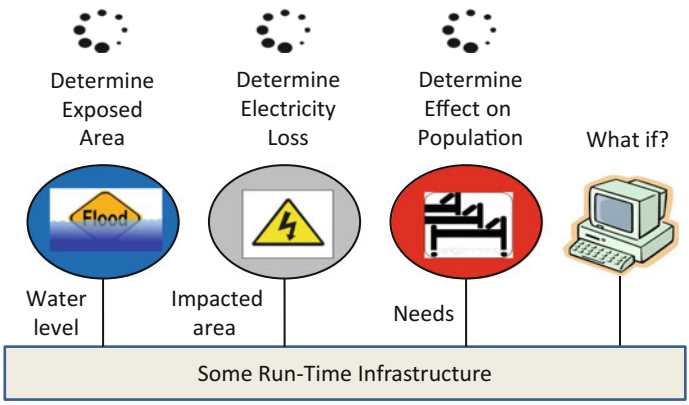


Fig. 1 Federated models through some run-time infrastructure

This chapter provides an overview of several standards that have been developed over time in the area of distributed (or federated) simulation. These standards address simulation interoperability as well as the engineering of distributed simulation environments.

The structure of this chapter is as follows:

- Section 2 starts with an introduction to distributed simulation and two main challenges, namely *interoperability* and *composability* of simulation models;
- Section 3 provides an overview of the *High Level Architecture* (HLA), an interoperability standard for distributed simulation;
- Section 4 introduces the *Distributed Simulation Engineering and Execution Process* (DSEEP), an engineering process to address the needs of a very large and diverse user community in the engineering of distributed simulation environments;
- Section 5 discusses the *Federation Agreements Template* (FEAT), a standardized format for recording simulation environment agreements to increase their usability and reuse;
- And lastly, Sect. 6 provides a summary.

2 Distributed Simulation

2.1 Introduction

Distributed simulation is a key technology in modern simulation systems and refers to the distributed execution of simulation models in a common synthetic environment. The simulation models may be located on a set of processing nodes in a local area network, or geographically spread across different processing nodes connected through a wide area network. The distributed simulation models execute together as if they were all combined on a single processing node.

Distributed simulation can contribute to cost-reduction by the reuse of simulation models, increase flexibility by exchanging simulation models, improve scalability, reduce execution times, include hardware or man in the loop that may be located elsewhere, include simulation assets that are tied to a certain location, improve quality through the reuse of validated simulation models, etc.

Two major challenges in distributed simulation are to achieve *interoperability* and *composability* of different simulation models, as discussed in the next section. These challenges are equally applicable to modeling and simulation for Critical Infrastructures.

2.2 Levels of Interoperability

Over the years the topics of interoperability and composability have been discussed in several papers. In [1] Petty defines interoperability as:

> the ability of different simulations, connected in a distributed simulation, to meaningfully collaborate to simulate a common scenario or virtual world

And composability as:

> the capability to select and assemble simulation components in various combinations into simulation systems to satisfy specific user requirements

Also, as stated in the same paper: Interoperability is necessary but not sufficient for composability. Composability *requires* interoperability, but interoperability is possible without composability, i.e., without the ability to combine and recombine. For example, two models A and B may be interoperable but it does not make sense to compose them together if their objectives and underlying assumptions are not aligned. E.g. the composition of an engine model that produces supersonic aircraft velocities and a flight dynamics model that is only valid for subsonic velocities, does not make sense although both models might be interoperable. An example of composability is shown in Fig. 2: LEGO building blocks are interoperable and composable.

In [2] Page et al. describe three dimensions to the simulation interconnection problem:

- *Composability*—realm of the model (e.g. two models are composable if their objectives and assumptions are properly aligned).
- *Interoperability*—realm of the software implementation of the model (e.g. are the data types consistent, have the little endian/big endian issues been addressed, etc.)

Fig. 2 Composability: objectives and underlying assumptions are aligned

- *Integratability*—realm of the site the simulation is running at (e.g. have the host tables been set up; are the NIC cards working properly).

To successfully achieve the cooperative execution of two or more models, each of these dimensions of the interconnection problem must be "solved".

Tolk defines in [3] five levels at which simulation models can interoperate. These levels are called Levels of Conceptual Interoperability (LCIM) between simulation models. In [4] these levels got expanded to the current seven Levels of Conceptual Interoperability between simulation models:

- Level 0: *no interoperability*.
- Level 1: *technical interoperability*: a communication protocol exists for exchanging data between participating systems. On this level, a communication infrastructure is established allowing systems to exchange bits and bytes, and the underlying networks and protocols are unambiguously defined.
- Level 2: *syntactic interoperability*: a common protocol to structure the data is used and the format of the information exchange is unambiguously defined. This layer defines structure.
- Level 3: *semantic interoperability*: a common information exchange reference model is used, the meaning of the data is shared and the content of the information exchange requests are unambiguously defined. This layer defines (word) meaning.
- Level 4: *pragmatic interoperability*: the interoperating systems are aware of the methods and procedures that each system is employing. The use of the data is understood by the participating systems and the context in which the information is exchanged is unambiguously defined. This layer puts the (word) meaning into context.
- Level 5: *dynamic interoperability*: the interoperating systems are able to comprehend the state changes that occur in the assumptions and constraints that each is making over time, and they are able to take advantage of those changes. When interested specifically in the effects of operations, this becomes increasingly important; the effect of the information exchange within the participating systems is unambiguously defined.
- Level 6: *conceptual interoperability*: the assumptions and constraints of the meaningful abstraction of reality are aligned. This requires that conceptual models are documented based on engineering methods enabling their interpretation and evaluation by other engineers.

The seven levels of the LCIM are shown in Fig. 3, including the three dimensions of the simulation interconnection problem listed alongside the levels.

On the left side of seven levels in Fig. 3 the three dimensions of the simulation interconnection problem are shown:

- Integratability (level 1): refers to the physical and technical connections between systems, which include hardware and firmware, and network protocols.

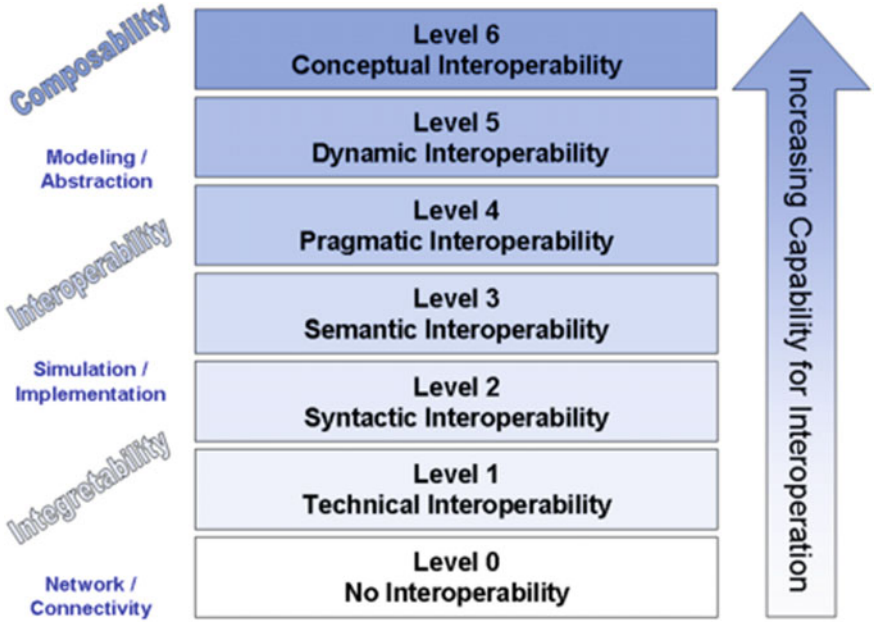


Fig. 3 Levels of conceptual interoperability model (LCIM)

- Interoperability (level 2–4): refers to the simulation and implementation details of interoperations, including exchange of data elements based on a common data interpretation.
- Composability (level 5–6): refers to the alignment of issues on the modeling level.

In [5] Wang et al. use the Levels of Conceptual Interoperability Model (LCIM) as a framework for conceptual modeling and for descriptive and prescriptive uses. In Table 1 the implications of the LCIM are listed, showing per level: premise, information and contents that should be defined, domain, focus, and capability to compose models.

In the same paper Wang et al. show how the LCIM can be used in a prescriptive role by providing the requirements that must be satisfied to reach a certain level of interoperability between simulation models, and engineering approaches on how to achieve that. The requirements and approaches are summarized in Table 2.

In Table 2 the High Level Architecture (HLA) is listed at levels 1–3. The HLA is a standard architecture for distributed simulation and is described in more detail in Sect. 3. According to the LCIM the HLA Runtime Infrastructure (RTI) is listed at level 1, providing technical interoperability between participating systems. The HLA Object Model Template (OMT) specification defines the structure of the information and is therefore at level 2. The HLA Real-time Platform Reference (RPR) Federation Object Model (FOM) is an example of a standard and reference object model that conforms to the HLA OMT specification, providing a common

Table 1 Implications of LCIM (adapted from [5])

Level	Premise	Information defined	Contents clearly defined	Domain	Focus	Capability
Level 6 Conceptual	Common conceptual model	Assumptions, constrains, etc.	Documented conceptual model	Modeling abstraction	Composability of models	High
Level 5 Dynamic	Common execution model	Effect of data	Effect of information exchanged			
Level 4 Pragmatic	Common workflow model	Use of data	Context of information exchanged	Simulation implementation	Interoperability of models	Medium
Level 3 Semantic	Common reference model	Meaning of data	Content of information exchanged			
Level 2 Syntactic	Common data structure	Structured data	Format of information exchanged			
Level 1 Technical	Common communication protocol	Bits and bytes	Symbols of information exchanged	Network connectivity	Integratability of models	Low
Level 0 No	No connection	NA	NA			

Table 2 Prescriptive role of LCIM (adapted from [5])

Level	Prescription of requirements to reach this level	Common reference engineering approaches
Level 6 Conceptual	A shared understanding of the conceptual model of a system (exposing its information, processes, states, and operations)	DoDAF; platform independent models of the MDA; SysML
Level 5 Dynamic	The means of producing and consuming the definitions of meaning and context is required	Ontology for Services; UML artifacts; DEVS; complete UML; BOM
Level 4 Pragmatic	A method for sharing meaning of terms and methods for anticipating context are required	Taxonomies; Ontology; UML artifacts, in particular sequence diagrams; DEVS; OWL; MDA
Level 3 Semantic	Agreement between all systems on a set of terms that grammatically satisfies the syntactic level solution requirements is required	Common reference model; dictionaries; glossaries; protocol data units; HLA RPR-FOM
Level 2 Syntactic	An agreed-to protocol that can be supported by the technical level solution is required	XML-XSD; HLA OMT; interface description language; WSDL
Level 1 Technical	Ability to produce and consume data in exchange with systems external to itself is required	Network connection standards such as HTTP; TCP/IP; UDP/IP, messaging middleware, such as HLA-RTI
Level 0 No	NA	NA

agreement for many participating systems [6]. The RPR-FOM is therefore at the semantic level 3. Simulation environment agreements (see Sect. 4, DSEEP step 4) —although not part of the HLA standard—are at the pragmatic level 4 when they capture the methods and procedures that each system is employing in using the data. However, at present simulation environment agreements tend to be mostly textual and a formal language such as UML, OWL or OWL-S is preferred to express agreements in order to reach a higher level of interoperability. As can be concluded from the LCIM, the HLA focuses on network connectivity as well as on simulation implementation, in particular on syntactic and semantic interoperability between simulation models. The HLA targets simulation interoperability, and, currently, much less simulation composability.

Another standard worth pointing out is Base Object Model (BOM) Template Specification [7] listed in Table 2 at level 5. The BOM Template Specification defines the format and syntax for describing a BOM. A BOM describes small parts of the interactions between simulation models as so called “patterns of interplay” together with a data model that is comparable to the concept of “FOM module” (described further in Sect. 3.4). The patterns of interplay are implementation independent descriptions of sequences of events between simulation entities. The BOM Template Specification can be used to describe the dynamic interoperability between simulation models at level 5.

2.3 Approach for Coupling Simulation Models

At the technical level of the LCIM (LCIM Level 1) two common approaches to federate simulation models are pairwise coupling and service bus coupling.

Pairwise coupling

Every simulation models connects to every other model as needed (see Fig. 4). For each connection a specific interface may need to be constructed, a dedicated data exchange model defined and operating agreements established. This approach may work fine for connecting just a few models, but obviously when the number of models grow also the number of connections grow rapidly! Furthermore, connections between models may become solution specific, thus hampering model reusability.

Service bus coupling

In this approach each simulation model has a common interface to a so called "service bus" (see Fig. 5). This bus provides standard simulation services that models may use to coordinate their activities, exchange data, and progress simulation time. Common topologies for a service bus are: centralized (communication between connected simulation models is via a central server component or broker) or decentralized (communication is directly between connected models), or a mix of these two. This approach has the advantage of limiting the number connections and interfaces and stimulating reuse of simulation models over time. Regardless of the topology, the simulation models use a common interface to communicate with each other. Often this common interface is realized by a software component called "run-time infrastructure".

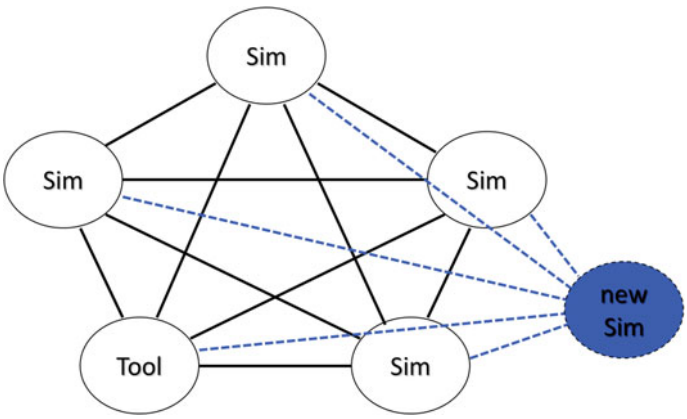


Fig. 4 Pairwise coupling

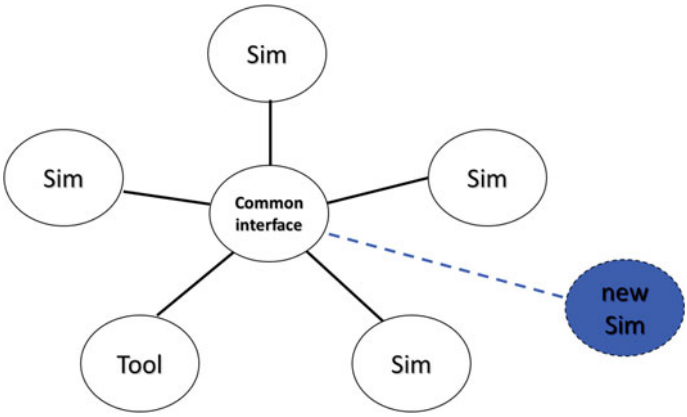


Fig. 5 Service bus coupling

The HLA is a general reference architecture for distributed simulation and defines a service bus for connecting simulation models (in HLA terminology these are called "federates"). The service bus is called the HLA Run Time Infrastructure (HLA-RTI). An overview of the HLA is provided in the next chapter.

3 Overview of the High Level Architecture

3.1 Introduction

The High Level Architecture (HLA) is an international standard for the development of distributed simulation environments. In the terminology of the HLA, individual simulation applications are known as federates. Federates may be simulation models, data collectors, simulators, computer generated forces or passive viewers. The collection of federates brought together to form a synthetic environment is known as a federation. It is the common interpretation of a shared data model, called the Federation Object Model (FOM), that allows federates to interact within a single synthetic environment. A federation execution refers to the process of conducting a distributed simulation. Federates interact via a Runtime Infrastructure (RTI). The RTI provides a number of Application Programming Interface (API) service groups that are used by a federate to interact with the underlying communication layer.

Figure 6 provides an example of an HLA federation, where simulators, support tools, and live participants interact through a common Runtime Infrastructure.

The HLA is focused on interoperability between various types of simulations, and to promote reuse of simulations and their components. The HLA follows two general design principles:

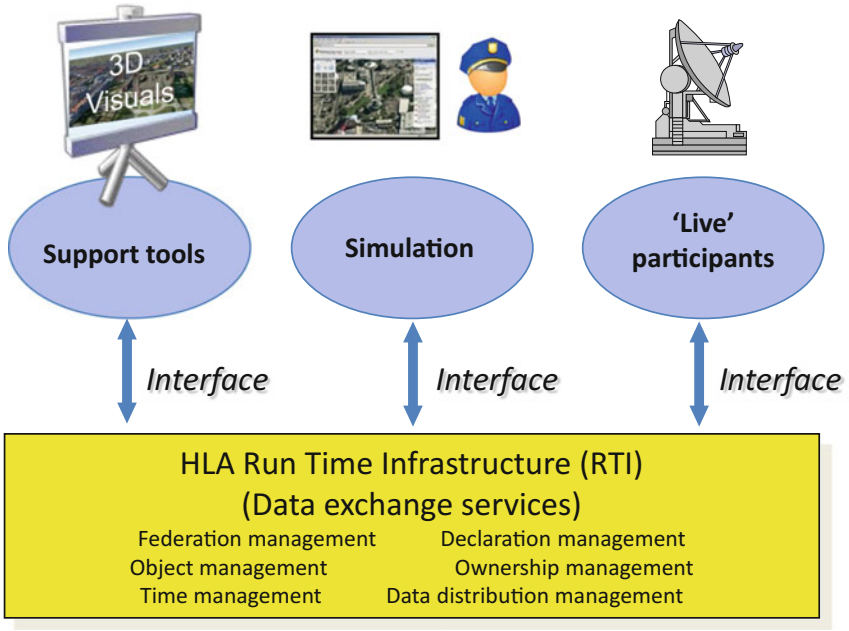


Fig. 6 A graphical view of the HLA: federates operate together through a common runtime infrastructure (RTI)

- *modularity*: simulation components (federates) are composed into larger systems (federations) to obtain a specific functional behavior;
- *separation of concerns*: the functional behavior of the components (federates) are separated from the supporting communication infrastructure (RTI) via a well-defined interface.

The HLA was originally developed for defense applications but there is a growing non-defense user base of the HLA. Numerous publications on HLA applications can be found via google scholar. A search on the publications from 2010 with keywords "HLA RTI" yields over 2700 hits, and shows a variety of topics such as warfare simulation, distributed-parallel computer simulations, cyber physical simulation, aircraft flight simulation, railway simulation, off-shore maritime simulation, engineering design analysis simulation, engine simulation, and lunar landing simulation.

The HLA is an international standard, developed and maintained by the Simulation Interoperability Standards Organization (SISO) and published by IEEE. The first complete version of the standard was published in 1998. It was known as "HLA 1.3". HLA became an IEEE standard (IEEE 1516) in 2000. The IEEE 1516 standard has been updated in 2010, and is known as "HLA Evolved".

The HLA standard is composed of three parts: the HLA Framework and Rules, the HLA Interface Specification, and the HLA Object Model Template (OMT) Specification:

- IEEE 1516-2010. HLA Framework and Rules: ten rules describing the responsibilities of federations and federates and their relationship with the RTI [8];
- IEEE 1516.1-2010. HLA Interface Specification: identifies how federates interact within the federation. In fact, it specifies the API (Application Programmer's Interface) of the HLA Run Time Infrastructure (HLA-RTI) [9];
- IEEE 1516.2-2010. HLA Object Model Template (OMT) Specification: provides a common format for describing all HLA objects and interactions, and establishes the syntax and format of the Federation Object Model (FOM) and Simulation Object Model (SOM) [10].

These parts are discussed in the following sections.

3.2 Framework and Rules

The HLA Framework and Rules [8] mandate a certain structure for federates and federations to ensure that the models are re-usable across applications.

There are 10 rules.

The rules for federations are in summary:

1. Federations shall have an HLA FOM, documented in accordance with the HLA OMT;
2. In a federation, all simulation-associated object instance representation shall be in the federates, not in the RTI;
3. During a federation execution, all exchange of FOM data among joined federates shall occur via the RTI;
4. During a federation execution, joined federates shall interact with the RTI in accordance with the HLA interface specification;
5. During a federation execution, an instance attribute shall be owned by at most one joined federate at any given time;

and the rules for federates are in summary:

1. Federates shall have an HLA SOM, documented in accordance with the HLA OMT;
2. Federates shall be able to update and/or reflect any instance attributes and send and/or receive interactions, as specified in their SOMs;
3. Federates shall be able to transfer and/or accept ownership of instance attributes dynamically during a federation execution, as specified in their SOMs;
4. Federates shall be able to vary the conditions (e.g., thresholds) under which they provide updates of instance attributes, as specified in their SOMs;
5. Federates shall be able to manage local time in a way that will allow them to coordinate data exchange with other members of a federation.

3.3 Interface Specification

The HLA Interface Specification [9] describes seven service groups which are used by the federate to interact with the underlying communication layer, called the Run Time Infrastructure (RTI). A service group is a term to refer to a collection of related interface calls to the RTI. All communications between the federates are processed through the RTI. The federates may give advice, or send requests to the RTI, and the RTI can respond asynchronously by invoking certain well-known call-back methods. A callback is a user-defined piece of software code (with a given interface) that is invoked by the RTI when a certain event occurs.

The seven service groups are in summary:

1. Federation Management. These services allow for the coordination of federation-wide activities throughout the life of a federation execution. Such services include federation execution creation and destruction, federate application joining and resigning, federation synchronization points, and save and restore operations. This can for example be used to create "snapshots" of the simulation in order to resume execution at a later stage.
2. Declaration Management. These services allow joined federates to specify the types of data they will supply to, or receive from, the federation execution. This process is done via a set of publication and subscription services along with some related services.
3. Object Management. These services support the life-cycle activities of the objects and interactions used by the joined federates of a federation execution. These services provide for registering and discovering object instances, updating and reflecting the instance attributes associated with these object instances, deleting or removing object instances as well as sending and receiving interactions and other related services. (Note: Formal definitions for each of these terms can be found in the definitions clause of all three HLA specifications.)
4. Ownership Management. These services are used to establish a specific joined federate's privilege to provide values for an object instance attribute as well as to facilitate dynamic transfer of this privilege (ownership) to other joined federates during a federation execution.
5. Time Management. These services allow joined federates to operate with a logical concept of time and to jointly maintain a distributed virtual clock. These services support discrete event simulations and assurance of causal ordering among events.
6. Data Distribution Management. These services allow joined federates to further specify the distribution conditions (beyond those provided via Declaration Management services) for the specific data they send or ask to receive during a federation execution. The RTI uses this information to route data from producers to consumers in a more tailored manner, for example to receive only updates from objects that are in the geographical vicinity in the simulated world.

7. Support Services. This group includes miscellaneous services utilized by joined federates for performing such actions as name-to-handle and handle-to-name transformations, the setting of advisory switches, region manipulations, and RTI start-up and shutdown.

The RTI services provide many ways to optimize the federation execution in terms of wall clock execution time and the amount of data exchanged. For example, via advanced time management schemes, object update rate reduction, data interest management, attribute ownership transfer, and data distribution management.

It is impossible to discuss all of these service specifics in the available space of this chapter. However, an overview of a typical usage of the services is discussed below.

The first service group that a federate will use is federation management.

The federation management services enable federates to join the federation as depicted in Fig. 7. A federate typically provides a list of FOM modules that it will use for communication.

Next, federates will need to declare their interest in the data described in the FOM or FOM modules, and tell the RTI what data they provide and consume. The declaration management services are used for this purpose. This is shown in Fig. 8.

To communicate with each other, federates use the object management services as depicted in Fig. 9. The object management services deal with the registration, modification, and deletion of object instances and the sending and receipt of interactions.

Messages (object instance updates and interactions) that federates exchange may be time managed. The RTI is responsible for keeping the federates time-synchronized.

A federate can ask the RTI if it is allowed to proceed in time. The RTI checks whether all other federates are ready to proceed. If so, it tells the federates with which Δt they can progress. A federate uses the RTI time management services to manage logical time and to ensure that the data that is exchanged with the object

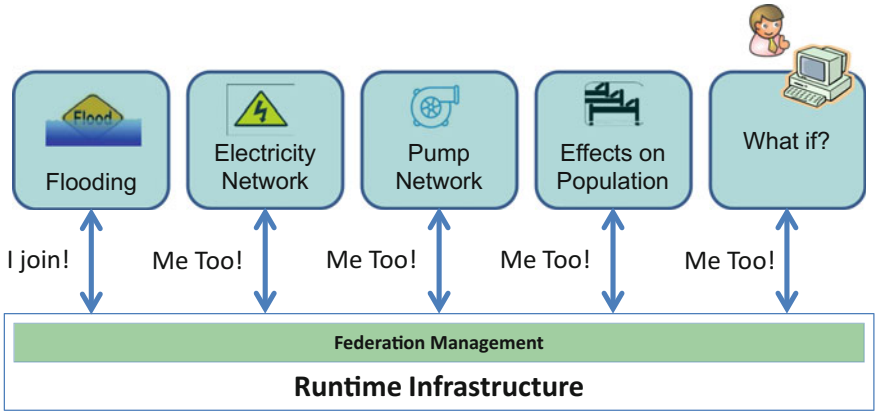


Fig. 7 Federates joining a federation

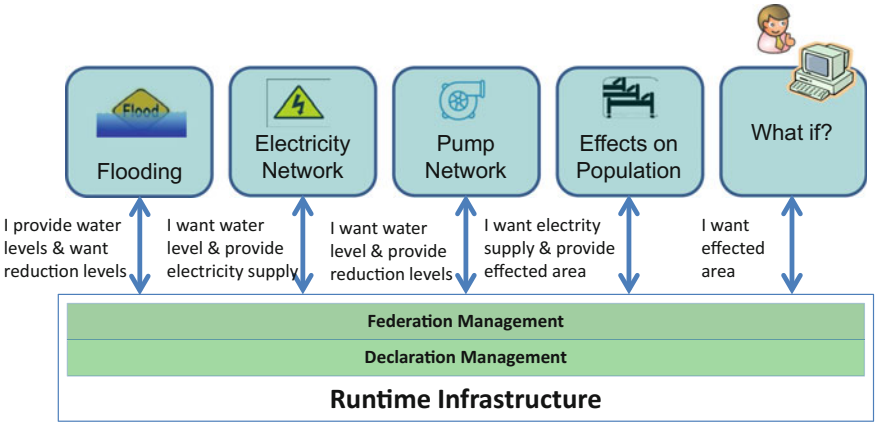


Fig. 8 Federates need to describe what data they provide/consume

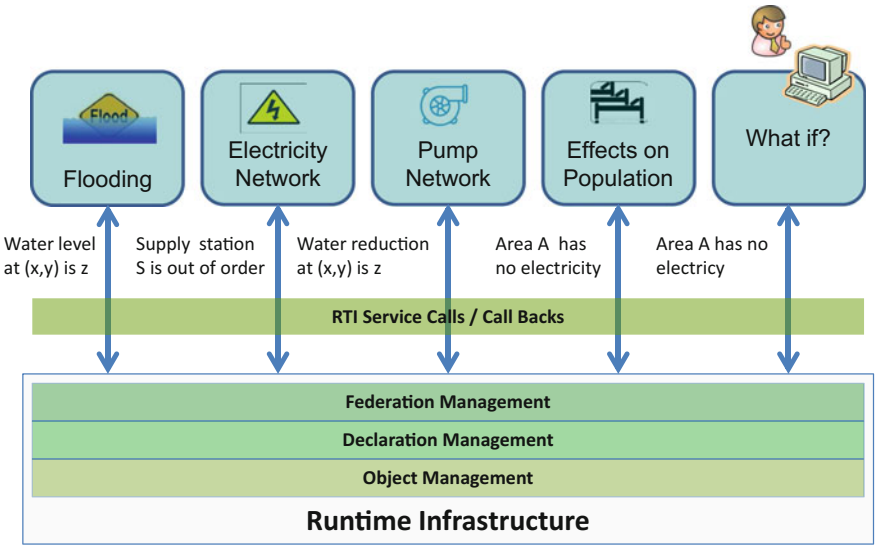


Fig. 9 Federates need to exchange data and interactions

management services is delivered at the correct logical time at other federates. Figure 10 provides an example what could happen if time is not synchronized; each federate progresses time at its own pace and the federates are all at a different logical time when they exchange date. The time management services support different ways to progress logical time (e.g. time stepped, event driven) and optimize time advancement and concurrency in federation execution.

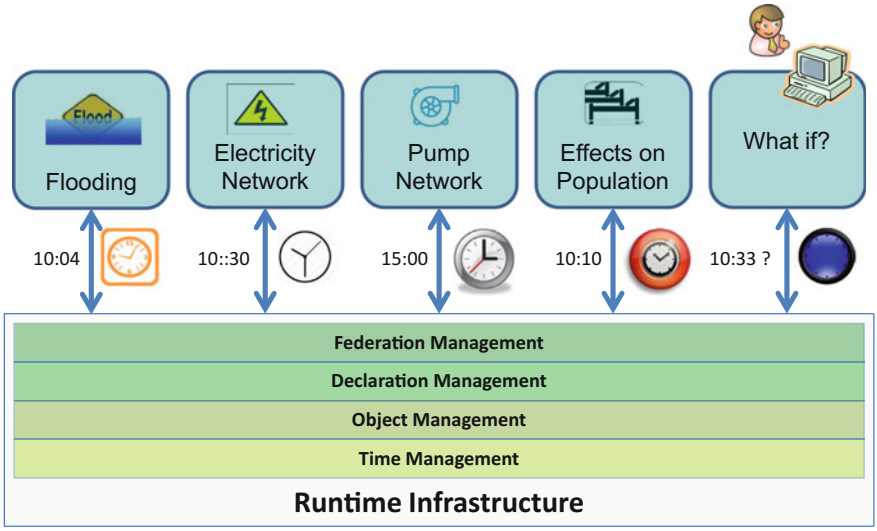


Fig. 10 Federate simulation time need to be synchronized

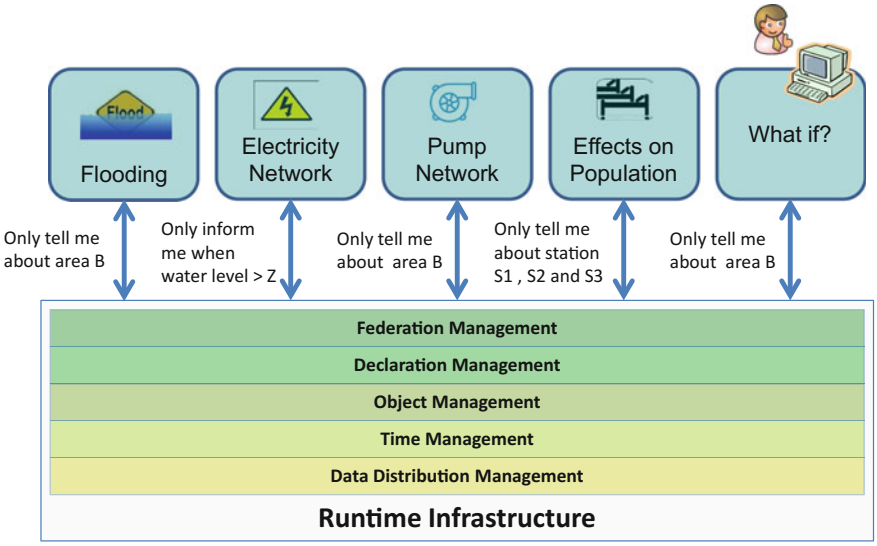


Fig. 11 Updating of information can be optimized

To increase scalability of a federation and performance of federates, updating of information can be optimized. As depicted in Fig. 11 a federate can instruct the RTI to forward only the information that is relevant for him. This mechanism reduces the work load on the federate: it doesn't have to process data that can be discarded anyway.

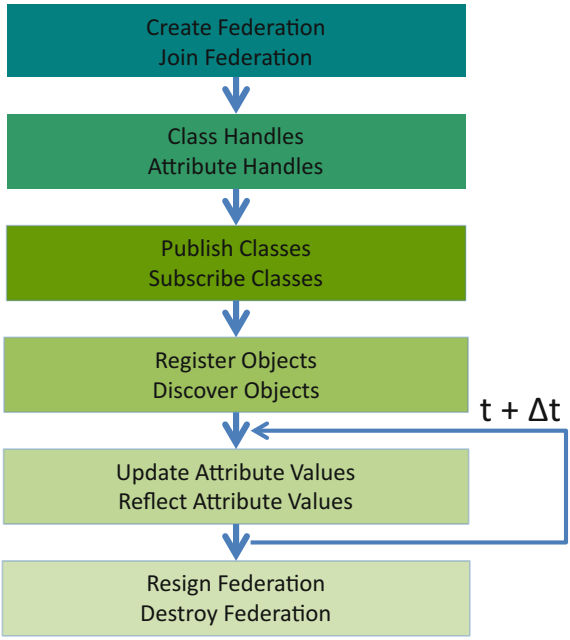


Fig. 12 Schematized HLA program walkthrough: lifecycle of a federation

Federates can internally use different concepts than specified in the FOM of the federation it wants to join, such as units. The FOM may specify distance in kilometers, whereas the federate internally uses meter as unit. Mapping of FOM attribute values to internal values is the responsibility of the joining federate.

Finally, Figs. 12 and 13 show a high level schema of the steps to create and execute a federated simulation. These are the typical steps performed in the lifecycle of a federation.

3.4 Object Model Template Specification

All possible data exchanged by federates in a federation is captured in an object model [10]. The object model may contain "HLA objects" to describe the persistent state of entities, and "HLA interactions" to describe transient events. The HLA-OMT provides a format for this object model. There are three kinds of such object models in the HLA framework: SOM, FOM and MOM.

An individual federate is described by its Simulation Object Model (SOM). The SOM is an object model in the HLA-OMT format that provides details of the object attributes and interactions that this federate either provides or receives information about.

All data that is potentially exchanged in a collection of federates (i.e., the federation) is described by the FOM. The FOM is also an object model in the

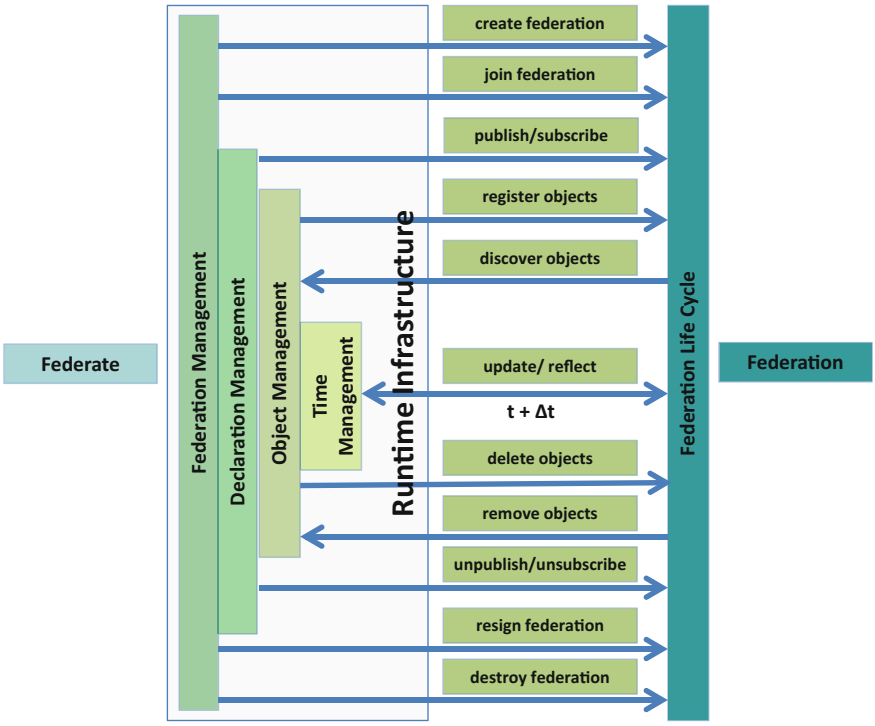
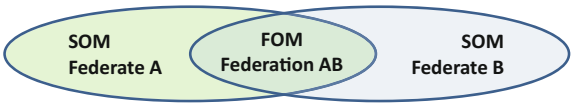


Fig. 13 Program walkthrough schema and interactions: lifecycle of a federation

Fig. 14 FOM and SOM



HLA-OMT format that contains all objects and interactions that the federates may exchange. Since all information is available in the individual SOMs, the FOM can be constructed out of the SOMs. In addition, the FOM may contain some federation-wide information for efficient data distribution management. Figure 14 provides an example of a FOM as an intersection of SOM A and SOM B.

The FOM and SOMs may be regarded as technical contracts that serve as interface specifications for the federate developers. A particular federate in a federation may be replaced by another version if it complies with the same SOM and federation agreements as the original federate.

A third object model is the Management Object Model (MOM). The MOM is a group of predefined constructs that provide support for monitoring and controlling a federation execution. A predefined FOM module, called MOM and Initialization Module (MIM), contains predefined HLA constructs such as object and interaction roots, data types, transportation types, and dimensions.

The FOM may be developed from the individual SOMs, but the use of a reference FOM is often a good starting point, as shown in Fig. 15. An example of a reference FOM is the RPR-FOM (Real-time Platform-level Reference FOM) [6]. The RPR-FOM is a reference FOM that defines HLA classes, attributes and parameters that are appropriate for real-time, platform-level simulations in the military domain.

The HLA does not mandate any particular Federation Object Model (FOM). HLA is intended to be a domain independent simulation framework. However, several "reference FOMs" have been developed to promote interoperability within a specific application domain. HLA federations must always agree on a common FOM (among other things), and reference FOMs provide ready-made FOMs that are supported by a wide variety of tools and federates. Reference FOMs can be used as-is, or can be extended to add new simulation concepts that are specific to a particular federation or simulation domain.

A new concept introduced in HLA Evolved is that of "FOM module". A FOM can consist of multiple FOM modules, each providing a part of the object model. The modularization of the FOM enables a number of things, for example (see also [11]):

- Different working groups can easily develop different parts of a FOM;
- Agreements related to a certain FOM module can be re-used between many federations;

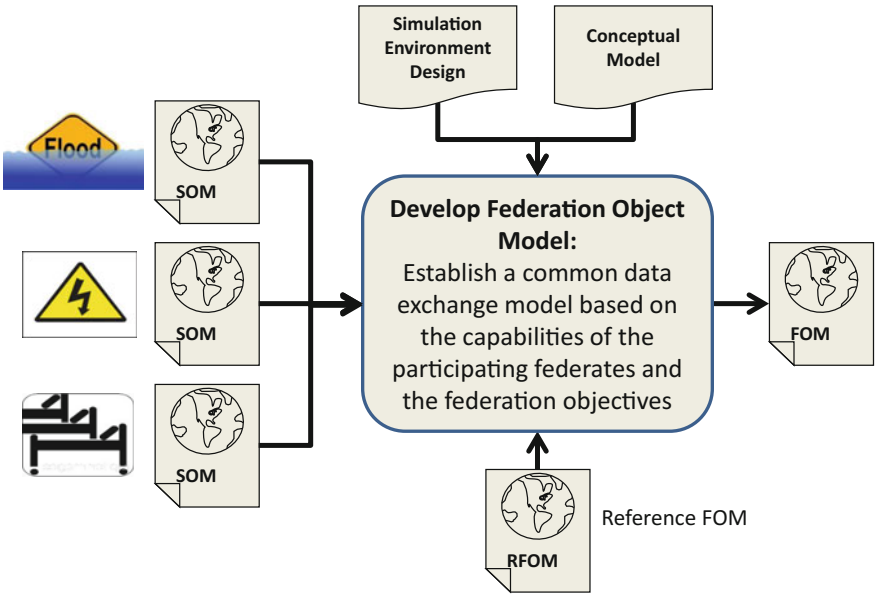


Fig. 15 Develop a federation object model

- Extensions to a reference FOM can be put in a FOM module to avoid modifying standard FOMs;
- New concepts to an already running federation can be added in new modules when new federates join;
- FOMs can become more agile as it is easy to add a new or change an existing FOM module that only some federates use;
- A service oriented approach is possible where a federate defines the provided service data in a FOM module;
- A more decentralized approach with self-organizing federates can be applied: only federates that use the same FOM module exchange data and need to make agreements between each other.

3.5 HLA RTI Implementations

A brief (and not up to date) overview of available HLA RTI implementations can be found on Wikipedia [12]. The most relevant implementations are listed in Table 3.

Pitch and MÅK are the two major competitors that provide an IEEE 1516-2010 compliant RTI, plus additional tools and professional services. Tools include gateways, object model template editors, code generators, data recorders, and visualization tools. The open source alternatives are all partial implementations and it is not always clear what functionality is lacking. For example, for poRTIco, there

Table 3 HLA RTI implementations

Vendor	URL	Standard	Binding	License
Pitch	http://pitch.se	HLA 1.3	C++, Java	Commercial
		IEEE 1516-2000	C++, Java	
		IEEE 1516-2010	C++, Java	
MÅK	http://www.mak.com	HLA 1.3	C++, Java	Commercial
		IEEE 1516-2000	C++, Java	
		IEEE 1516-2010	C++, Java	
CERTI	http://savannah.nongnu.org/projects/certi	HLA 1.3 (partial)	C++, Java	Open source: GPL (sources) and LGPL (libraries)
		IEEE 1516-2000 (partial)	C++	
		IEEE 1516-2010 (partial)	C++	
poRTIco	http://porticoproject.org	HLA 1.3 (partial)	C++, Java	Open source: CDDL 1.0
		IEEE 1516-2000 (partial)	C++	
		IEEE 1516-2010 (partial)	C++, Java	

(continued)

Table 3 (continued)

Vendor	URL	Standard	Binding	License
Open HLA	http://sourceforge.net/projects/ohla	HLA 1.3 (partial)	Java	Open source: Apache Licence 2.0
		IEEE 1516-2000 (partial)	Java	
		IEEE 1516-2010 (partial)	Java	

is no MOM support, but most other HLA Evolved services appear to be implemented. In general, the CERTI RTI and poRTIco RTI are mature open source implementations and form a good alternative for the commercial RTI implementations.

An HLA tutorial with accompanying materials (sample federates, FOMs, RTI) can be found on the Pitch website. MÅK also provides a tutorial and a free RTI for two federates on their website. Several organizations (e.g. SISO) offer training courses, documentation etc.

4 Distributed Simulation Environment Development

As distributed simulations become more complex, and tend to be systems in their own right, a structured systems engineering approach is needed to develop and maintain them. Although traditional software development processes may be applied to the development of distributed simulation environments, these processes lack simulation specific steps and activities that are important for distributed simulation environments. For example, the development of a simulation conceptual model and simulation scenario, and the development of a simulation data exchange model with associated operating agreements between member applications. The only recognized industry standard process for distributed simulation environment development is described in [13], called Distributed Simulation Engineering and Execution Process (DSEEP). This process is independent of a particular simulation environment architecture (e.g. HLA) and provides a consistent approach for objectives definition, conceptual analysis, design and development, integration and test, simulation execution, and finally data analysis.

The DSEEP was originally developed under the umbrella of the Simulation Interoperability Standards Organization (SISO) by a large community of (distributed) simulation practitioners, and became an IEEE standard in 2010. A top-level illustration of this process is provided in Fig. 16. The DSEEP identifies a sequence of seven basic steps with activities to design, develop, integrate, and test a distributed simulation environment of disparate simulation models. Each activity in the DSEEP is further broken down in tasks and work products. The guidance provided by the DSEEP is generally applicable to standalone simulations as well.

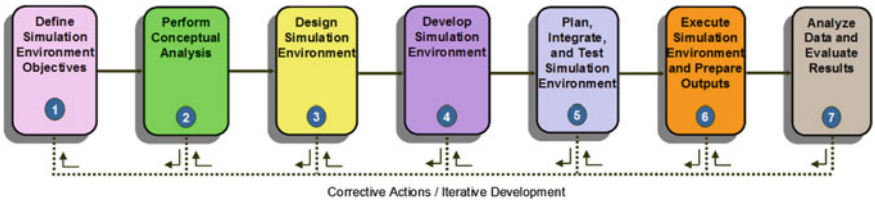


Fig. 16 DSEEP seven step process

A brief summary of each step of the DSEEP is provided below. For more information the reader is referred to the standard itself.

The DSEEP steps are:

Step 1 Define simulation environment objectives. Define and document a set of needs that are to be addressed through the development and execution of a simulation environment and transform these needs into a more detailed list of specific objectives for that environment. Measures of effectiveness (MOEs) and measures of performance (MOPs) are important factors in defining the simulation environment objectives. MOEs and MOPs will be reflected in the simulation models, the data that is exchanged through the FOM and the data that should be captured for analysis. Step 1 will typically also consider the constraints that apply to the simulation design and execution, for example simulation systems that must be included or used for certain aspects of the problem, schedules, costs, etc.

Step 2 Perform conceptual analysis. Develop an appropriate representation of the real-world domain that applies to the defined problem space and develop the appropriate scenario. It is also in this step that the objectives for the simulation environment are transformed into a set of simulation environment requirements that will be used for simulation environment design, development, testing, execution, and evaluation.

One important output of this step is a conceptual model. The conceptual model describes amongst others the relevant entities within the domain of interest, describes the static and dynamic relationships between entities, and describes the behavioral and transformational (algorithmic) aspects of each entity. The role of the conceptual model is illustrated in Fig. 17. The conceptual model defines the "abstraction level" or "simplification" of the real world that is appropriate for the problem at hand.

Another important output of this step is a scenario. The scenario includes the types and numbers of major entities that must be represented within the simulation environment, a functional description of the capabilities, behavior, and relationships between these major entities over time, and a specification of relevant environmental conditions (such as urban terrain versus natural area, type of terrain, day/night, climate, etc.) that impact or are impacted by entities in the simulation environment. Initial conditions

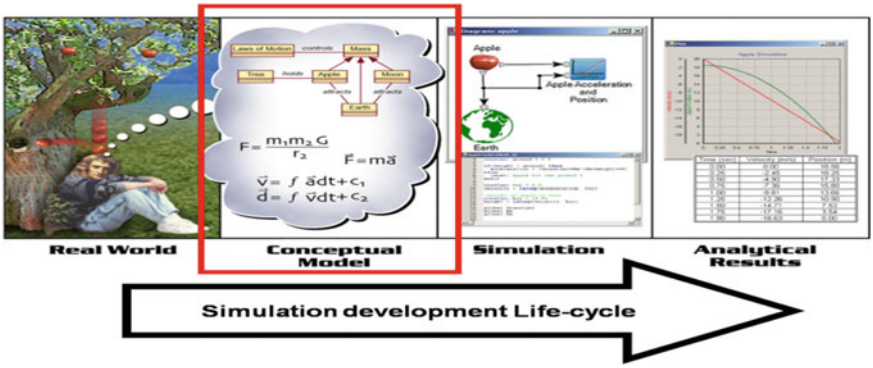


Fig. 17 The role of the conceptual model in the Simulation development life-cycle [14]

(e.g., geographical positions for physical objects), termination conditions, and specific geographic regions should also be provided.

A third important output of this step is the requirements for the simulation environment. This includes requirements for properties and behaviors that the simulation environment must represent, requirements for fidelity, as well as more technical requirements.

Step 3 Design simulation environment. Produce the design of the simulation environment that will be implemented in Step 4. This involves identifying member applications that will assume some defined role in the simulation environment (in HLA these are called federates) that are suitable for reuse, creating new member applications if required, allocating the required functionality to the member application representatives.

This step may include trade-off analysis to select the most appropriate member applications. Important outputs of this step include a list of member applications, allocated responsibilities, requirements gaps, and the simulation environment architecture.

Step 4 Develop simulation environment. Define the information that will be exchanged at runtime during the execution of the simulation environment, establish interface agreements, modify existing or develop new member applications (including models) if necessary, and prepare the simulation environment for integration and test.

Two important outputs of this step are a Simulation Data Exchange Model (SDEM) and simulation environment agreements. The Simulation Data Exchange Model describes the data that member applications can exchange at runtime (for HLA this corresponds to the FOM). Although the SDEM represents an agreement among member applications as to how runtime interaction will take place, there are other operating agreements that must be reached that are not documented in the SDEM. Such agreements are necessary to establish a fully consistent, interoperable, simulation environment. There are many different types of agreements, for instance, agreements on

initialization procedures, synchronization points, save/restore policies, progression of time, object ownership, attribute update policies, security procedures, as well as algorithms that must be common across the simulation environment to achieve valid interactions among all member applications.

Step 5 Integrate and test simulation environment. Integration activities are performed, and testing is conducted to verify that interoperability requirements are being met.

Step 6 Execute simulation. The simulation is executed and the output data from the execution is pre-processed.

Step 7 Analyze data and evaluate results. The output data from the execution is analyzed and evaluated, and results are reported back to the user/sponsor.

The standard also includes a number of "overlays" for existing distributed simulation environment architectures such as DIS and HLA.

In the light of the LCIM described in Sect. 2, DSEEP steps 1–4 are of great importance. In these four steps the objectives, the conceptual model, the simulation environment design, and the simulation data exchange model and operating agreements, are developed. These are all important elements in the LCIM.

A more rigorous systems engineering approach to architecture development (and to achieving a higher level of interoperability) in these four steps is described in [15], "Simulation environment architecture development using the DoDAF". This paper examines the application of US Department of Defense (DoD) Architecture Framework (DoDAF) and the related systems engineering concepts in simulation environment architecture development. In this approach the simulation environment is described using different, but interrelated, architectural viewpoints as shown in Fig. 18. Each architecture viewpoint defines several kinds of (UML) models (not to be confused with simulation models) to represent aspects of the system. The Operational Viewpoint, for example, is used in the Conceptual Analysis step of the DSEEP and defines model kinds for the description of operational activities and performers, workflow, information flow, and event traces for operational scenarios (in this case related to crtitical infrastructures). These models provide an implementation-independent representation of the systems and processes that the simulation environment must model and form one of the inputs to the simulation environment design.

While the DoDAF was not targeted for simulation environment development, the architectural constructs described by the DoDAF show great promise in terms of applicability to the simulation domain. By reusing these constructs, users may leverage a very broad and deep knowledge base of systems engineering experience to facilitate more capable and robust simulation environments in the future. The approach in this paper can be used to develop and document the conceptual model in a systematic way and achieve a higher level of interoperability between simulation models.

To summarize, the DSEEP is intended as a higher-level framework into which low-level management and systems engineering practices native to user organizations can and should be integrated. In general, this framework will have to be tailored to become a practical and beneficial tool for both existing and new

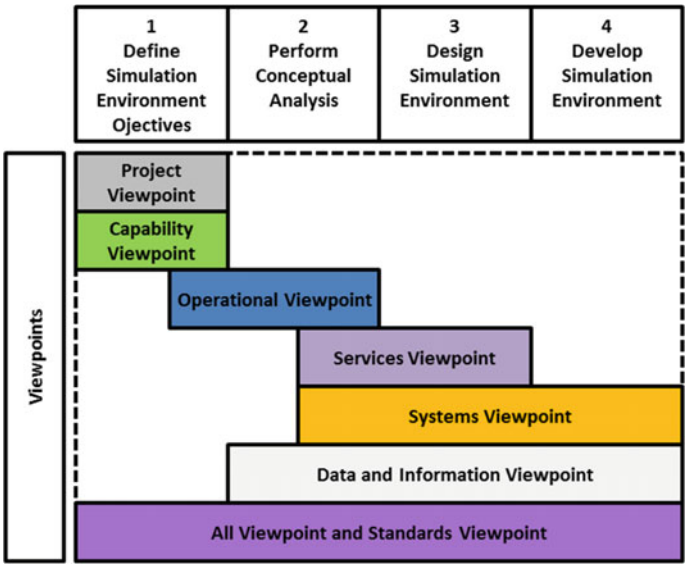


Fig. 18 DoDAF viewpoints per DSEEP step

simulation developments. The intent of the DSEEP is to specify a set of guidelines for the development and execution of these environments that stakeholders can leverage to achieve the needs of their application.

5 Federation Agreements Template

The Federation Engineering Agreements Template (FEAT) is intended to provide a standardized format for recording simulation environment agreements (see DSEEP step 4) to increase their usability and reuse. The template is an eXtensible Markup Language (XML) schema from which compliant XML-based simulation environment agreement documents can be created. XML was chosen for encoding agreements documents because it is both human and machine-readable and has wide tool support. Creating the template as an XML schema allows XML-enabled tools to both validate conformant documents, and edit and exchange agreements documents without introducing incompatibilities. Many of the artefacts generated in the DSEEP can be recorded using the FEAT.

The schema has been developed by the SISO and is published at [16]. The top level schema elements are shown in Fig. 19.

The federation agreements are decomposed into the following eight categories:

1. Metadata—Information about the federation agreements document itself.
2. Design—Agreements about the basic purpose and design of the federation.

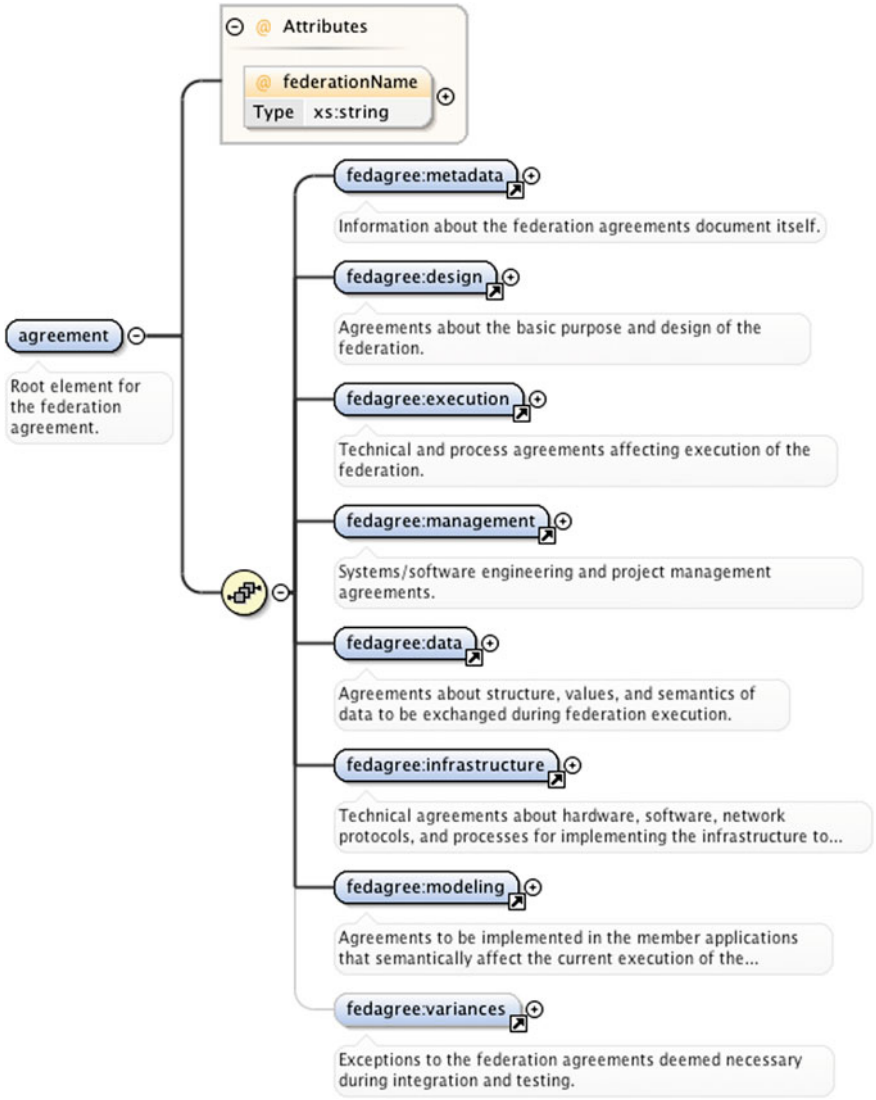


Fig. 19 FEAT top level schema elements

3. Execution—Technical and process agreements affecting execution of the federation.
4. Management—Systems/software engineering and project management agreements.
5. Data—Agreements about structure, values, and semantics of data to be exchanged during federation execution.

6. Infrastructure—Technical agreements about hardware, software, network protocols, and processes for implementing the infrastructure to support federation execution.
7. Modeling—Agreements to be implemented in the member applications that semantically affect the current execution of the federation.
8. Variances—Exceptions to the federation agreements deemed necessary during integration and testing.

Each category in the FEAT schema provides numerous elements that describe information that may be captured for a simulation environment. For example, Verification, Validation and Accreditation (VV&A) artefacts, Test artefacts, Security information, Member application data, objectives and requirements, hardware configurations, etc.

6 Summary

Modeling and Simulation (M&S) has become a critical technology in many domains. A set of coherent principles and standards are required to fully exploit the potential of M&S. Interoperability and composability are two challenges when federating simulation models. The seven Levels of Conceptual Interoperability (LCIM) between simulation models can be used to determine the level of interoperability between simulation models.

Federated simulations offer many advantages with respect to developing, using and maintaining complex simulation systems. The HLA offers a high quality standardised approach to federated simulation, supported by documentation, tools and an active user community. The advantages of open standards are:

- Economy of Scale;
- Comply with legislation;
- Promote Interoperability;
- Promote Common Understanding;
- Introduce Innovations, Transfer Research Results;
- Encourage Competition;
- Facilitate Trade.

The challenges of common standards also need to be addressed:

- Achieving consensus takes time. A user community must be established;
- Not-Invented-Here syndrome needs to be overcome by involving all stakeholders;
- Openness/Vendor Lock-In should be considered when selecting tools and suppliers;
- Maintenance of standards must be considered to ensure progress and prevent loss of investment.

Simulation practitioners should use their limited resources to focus on their domain specific needs (simulation models, simulation data exchange models,

simulation environment agreements, and verification methods) and benefit from existing tools and knowledge bases. I.e. focus on at least semantic interoperability between simulation models in a certain problem domain, and leverage existing standardised simulation middleware for the technical interoperability.

Acknowledgement and Disclaimer This chapter was derived from the FP7 project CIPRNet, which has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no. 312450.

The contents of this chapter do not necessarily reflect the official opinion of the European Union. Responsibility for the information and views expressed herein lies entirely with the author(s).

References

1. Petty M, Weisel E (2003) A composability lexicon (03S-SIW-023). In: SISO simulation interoperability workshop, Kissimmee, FL
2. Page E, Briggs R, Tufarolo J (2004) Toward a family of maturity models for the simulation interconnection problem (04S-SIW-145). In: SISO simulation interoperability workshop, Arlington, VA
3. Tolk A, Muguira J (2003) The levels of conceptual interoperability model (03S-SIW-007). In: SISO simulation interoperability workshop, Orlando, FL
4. Turnitsa CD (2005) Extending the levels of conceptual interoperability. In: Proceedings IEEE summer computer simulation conference, IEEE CS Press
5. Wang W, Tolk A, Wang W (2009) The levels of conceptual interoperability model: applying systems engineering principles to M&S. In: Spring simulation multiconference, San Diego, CA, USA
6. SISO (2015) Standard for guidance, rationale, and interoperability modalities (GRIM) for the real-time platform reference federation object model (RPR FOM), Version 2.0 (SISO-STD-001-2015), SISO
7. SISO (2006) Standard for base object model (BOM) template specification (SISO-STD-003-2006), SISO
8. IEEE (2010) IEEE standard for modeling and simulation (M&S) high level architecture (HLA)—framework and rules (IEEE 1516-2010), IEEE
9. IEEE (2010) IEEE standard for modeling and simulation (M&S) high level architecture (HLA)—federate interface specification (IEEE 1516.1-2010), IEEE
10. IEEE (2010) IEEE standard for modeling and simulation (M&S) high level architecture (HLA)—object model template (IEEE 1516.2-2010), IEEE
11. Möller B (2007) An overview of the HLA evolved modular FOMs (07S-SIW-108). In: SISO simulation interoperability workshop, Norfolk, VA
12. Run-time infrastructure (simulation) (2016) Wikipedia, 2016. Available: http://en.wikipedia.org/wiki/Run-time_infrastructure_(simulation). Accessed 2016
13. IEEE (2010) IEEE recommended practice for distributed simulation engineering and execution process (DSEEP) (IEEE 1730-2010), IEEE
14. Conceptual modeling (CM) for military modeling and simulation (M&S) (RTO-TR-MSG-058), NATO Science and Technology Organization, 2012
15. Berg T, Lutz R (2015) Simulation environment architecture development using the DoDAF (15F-SIW-019). In: SISO simulation interoperability workshop, Orlando, FL
16. SISO (2013) SISO federation engineering agreements template (FEAT) programmer's reference guide. Available: http://www.sisostds.org/FEATProgrammersReference

Author Biographies

Wim Huiskamp is Chief Scientist Modelling, Simulation and Gaming in the M&S department at TNO Defence, Security and Safety in the Netherlands. His research areas include system architecture, distributed real-time simulation and C2-Simulation interoperability problems. Wim acted as project lead for several national and international simulation (interoperability) projects and he currently leads the national simulation research program carried out on behalf of the Dutch MoD. In recent years Wim was the chairman of the NATO Modelling and Simulation Group (NMSG) and formerly also the chairman of the NMSG M&S Standards Subgroup (MS3). Wim is the liaison of the NMSG to the Simulation Interoperability Standards Organization (SISO).

Tom van den Berg is a senior scientist in the Modeling, Simulation and Gaming department at TNO, The Netherlands. He holds an M.Sc. degree in Mathematics and Computing Science from Delft Technical University and has over 25 years of experience in distributed operating systems, database systems, and simulation systems. His research area includes simulation systems engineering, distributed simulation architectures, systems of systems, and concept development and experimentation.

Chapter 7
Cyber Threats Impacting Critical Infrastructures

Michał Choraś, Rafał Kozik, Adam Flizikowski, Witold Hołubowicz and Rafał Renk

Abstract Nowadays it is important to note that security of critical infrastructures and enterprises consists of two factors, those are cyber security and physical security. It is important to emphasise that those factors cannot be considered separately and that the comprehensive cyber-physical approach is needed. In this paper we analyse different methods, methodologies and tools suits that allows modelling different cyber security aspects of critical infrastructures. Moreover, we provide an overview of goals an challenges, an overview of case studies (which show an increasing complexity of cyber physical systems), taxonomies of cyber threats, and the analysis of ongoing actions trying to comprehend and address cyber aspects.

1 Introduction

The CPS abbreviation stands for Cyber-Physical Systems and it refers to systems that have distributed natures, are comprised of physical elements that work in a real-time and are capable of communicating with each other by means of communication network (both wired and wireless, see Fig. 1). CPS integrate computational, communication and physical aspects in order to improve usability, efficiency, reliability, etc. However, such combinations, introduce a wide spectrum of risks related to cyber domain (e.g. privacy issues, cyber attacks).

The CPS are comprised of elements that allow for reading relevant information about controlled physical process (e.g. sensor) and elements that allows for influencing (via actuators) the behaviour of this process. The CPS are widely adapted in many critical sectors including energy, water, and transportation as well as in the area of smart houses, vehicles, etc.

M. Choraś (✉) · R. Kozik · A. Flizikowski · W. Hołubowicz · R. Renk
Institute of Telecommunications and Computer Science,
UTP University of Science and Technology, Bydgoszcz, Poland
e-mail: chorasm@utp.edu.pl

W. Hołubowicz · R. Renk
Adam Mickiewicz University, Poznań, Poland

R. Setola et al. (eds.), *Managing the Complexity of Critical Infrastructures*,
Studies in Systems, Decision and Control 90,
DOI 10.1007/978-3-319-51043-9_7

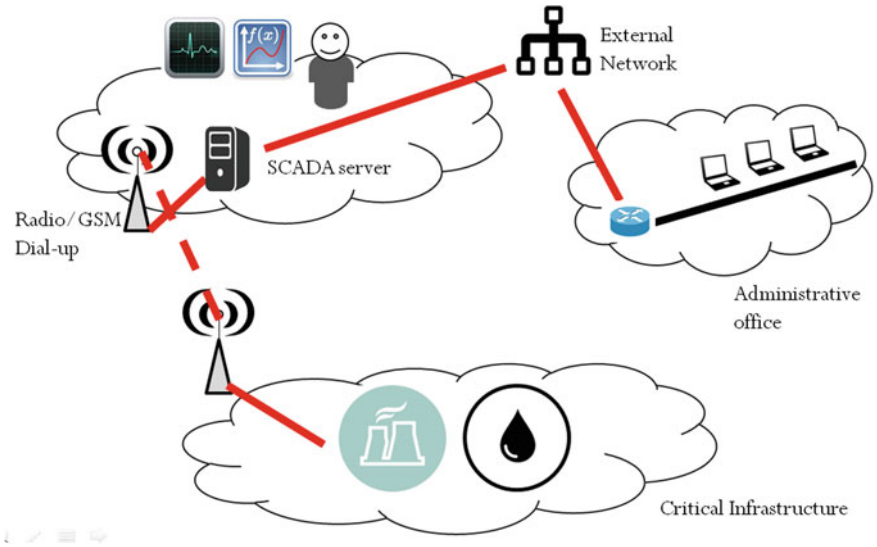


Fig. 1 Dependencies between complex systems comprising CPS

Currently, the CPS are on the direction to become an integral part of our lives, embracing in the near future such aspects as healthcare, disaster recovery, engineering, traffic control, robotic surgery, sea and space exploration, defence and military operations.

This paper is structured as follows: firstly, we analyse goals and challenges in area of cyber security of critical infrastructures, presenting case study overview and elaborating on the impact of the cyber domain on the real world. Next, we provide short overview of the taxonomies used to model and to analyse the cyber threats. Afterwards, we provide an general overview on how the cyber security life-cycle is modelled in terms of crisis management and critical infrastructures protection. Particularly, we focus on different approaches to cyber risk identification and cyber incidents handling. In the following section, we present different aspects of IT and physical networks that can be modelled with the formal tools and methodologies. The analysis of ongoing actions trying to comprehend and address the challenges of cyber aspects of critical infrastructures as well as the conclusions are given afterwards.

2 Goals and Challenges

Quantitative evaluation of cyber security is always a challenge in the area of computer science. For the CPS, the integration of ICT technologies with physical elements has introduced new threats. Currently, we may find many examples of the

attackers have been able to compromise complex systems by finding vulnerable elements. In many cases those attacks have had direct impact on physical elements. Therefore, there is an ongoing effort to embrace the cyber aspects of CPS with comprehensive tools and methodologies that commonly leverage wide spectrum of technical and non-technical means. The current challenges related to CPS can fall into following groups of problems:

- Security,
- Scalability,
- Complexity,
- Subsystems interoperability.

Of course, such problems should be handled in the holistic manner, e.g. by the THOR (Technical, Human, Regulatory, Organizational) approach and aspects as proposed by recently finished European projects [1, 2].

As the cyber security of CPS systems imposes a significant challenge, in this section, we particularly focus on different aspects of the cyber domain. We start with examples of case studies that in many cases reveal the complex nature of those systems and huge amount of interconnections that span across different levels of Critical Infrastructure management.

Afterwards, we provide examples of how the European Union addresses current problems and the challenges in the H2020 work program.

2.1 Cyber World and Real Impact—Selected Case Studies

Due to the fact that the energy sector is quickly evolving and it is widely adapting different ICT technologies, we are able to identify many high profile cyber incidents. One of the most important cyber attacks in history of Critical Infrastructures happened in 2012 [3], when Iran authorities announced that computers controlling one of its nuclear processing facilities had been infected with malicious software called Stuxnet. It was the first case in which industrial equipment was a target of computer attack. Since that date, the cyber community has realised that cyber weapon can be used "… to create physical destruction […] in someone else's critical infrastructure…" [4].

Also for the water sector, we are able to find relevant cyber incidents, which show a real and high impact of the cyber world on physical infrastructures. Similarly as for Energy sector, the cyber components for both drinking water and wastewater facilities include control systems known as Supervisory Control and Data Acquisition (SCADA) systems. Cyber attacks on such utilities may cause cascading effect on a public health, economics, and nations as whole. An example presented in [5] shows how the attacker can influence water treatment plants. According to IBTimes [5], attackers infiltrated the water plant and were able to change the level chemicals that were used to treat drinking water.

Healthcare industry is also an important part of critical infrastructure. It is also targeted by cyber criminals. As examples show [6, 7], cyber-attacks targeted at this sector can slow down hospitals and expose patients to danger.

Also the financial sector is struggling with cyber attack. According to [8] the activity of cyber criminals increased by 41% in recent years. Recent example of Bangladesh bank [9] show that attackers have effective tools and skills to infiltrate bank institutions and to steal serious amounts of money.

According to the [10], also the growth of the Internet of Things and complexity of industrial control systems will lead to more vulnerabilities in hardware systems. Many companies dealing with cyber security [1] have identified serious vulnerabilities in automotive systems and home-automotive systems. This shows that not only critical infrastructures but also citizens directly are currently impacted by the attackers as the cyber domain embraces increasing number of our lives.

2.2 The Coordinated Cyber Attack—Ukrainian Case

On the 23rd December 2015, the Ukrainian power distribution operator Prykarpattya Oblenergo was suffered attack on their ICT infrastructure performed by the third party. In effect of this breach, operation of a number of power substations were interrupted and about 80 thousands of customers from Ivano-Frankivsk region were suffered an outage for next three to six hours, according to the official information published through the operator website. At the same time, the operator informed publicity about other technical failure related to the operation of the call centre infrastructure. This caused impossibility for the customers to contact operator during the blackout and deepened the crisis.

The above described circumstances indicate that the energy operator faced the well-coordinated attack, that can be decomposed into three elements: a malware attack, a denial of service attack targeted at the call centre functionalities and the opening of substation breakers to cause the outage.

Firstly, the attackers infected the main servers controlling the electricity distribution process, they infiltrated in the victim's network (possibly using a malware backdoor) and issued a command to open breakers of various substations.

The goal of the cyber criminal was to enter the power grid system by infecting the victim's machines with malware software. They used macro script in Excel files to drop the malware. The infected Excel spreadsheets have been distributed during a spear-phishing campaign that targeted IT staff and system administrators working for multiple companies responsible for distributing electricity throughout Ukraine.

After the power was cut off, DoS attacks were launched to limit the target's awareness of the consequences of the attack—error messages did not reach service personnel what prevented from proper reaction on the crisis and delayed the recovering of the infrastructure operation.

The Ukrainian blackout case can be seen as the one of the first significant and publicly reported cyber attacks aimed at civil infrastructure and directly impacting

civil population (e.g. in opposition to the Stuxnet, Iranian case, where industry/military premises were infected). Ukrainian case shows that motivated attackers are able to cause serious damages to the economy and public safety of countries.

In case of the Ukrainian grid, luckily at that time, the manual mechanical reaction was possible. It would rather not be possible in case of the much modern and automated energy grids in some other countries.

2.3 Hybrid Conflicts

The Ukrainian case (described in the previous subsection) gives the short glance at the possible impacts of the successful cyber attack launched at the critical infrastructure such as energy grid. Unfortunately, due to the current geo-political situation and the current market of hackers (state and non-state), there is a significant threat that a country or its critical infrastructure can be attacked by another country or hackers organization working for another hostile country. It is worth to notice, that nowadays most hackers work for organizations rather than on their own (it changed significantly since in the past there were more freelancers than hackers working for organizations). In other words, cyber attacks might be a part of so called hybrid war or hybrid conflict, where (at least at the first stages) traditional military measures (such as soldiers) are not used, but the focus is on other destabilizing aspects like cyber attacks, cyber propaganda, influencing social media and electronic media etc. If the worst scenarios become reality, the successful coordinated cyber attacks launched at critical infrastructures such as banks (no possibility to draw money from ATM), energy (no electricity), transport, media etc. could paralyze societies, countries and create chaos.

Therefore, in order to avoid situation like in the Ukraine, the effective solutions and techniques to protect cyber physical systems are needed. The created recommendations and technologies should cover the wide spectrum of aspects, such as technological, organizational, human and regulatory (similarly to the THOR approach suggested by the new cyber roadmaps by projects like CAMINO, COURAGE and CyberRoad) [2, 11].

3 Cyber Threats Taxonomies

An important part of CPS cyber threats modelling is the taxonomy of cyber threats. To combat the cyber crime effectively, it is required to identify, define and classify the problem. It is not a trivial task, and currently even the spelling of the related words is not agreed, some use cybersecurity or cyber security or cyber-security. Similarly with other words like cybercrime, cyberterrorism etc.

A taxonomy is most often defined as a classification of terms and has close a relationship with the use of ontology. The primary purpose of ontologies and taxonomies is to use them as the basis for processing, communicating and reasoning about the cyber-related aspects and threats.

Also as noted by Furnell [12], having a consistent classification of cyber crime is beneficial for bodies and organisations interested in cyber counterterrorism. One of the earliest cyber crime classifications was established by UK Audit Commission and proposed in [13]. This categorisation identifies different groups of cyber crime activities, like: Fraud (for private gain of benefits), Viruses, Theft (of data or software), Use of unlicensed software, Hacking, Sabotage, Misuse of personal data, Introducing pornographic material.

In Furnell [12] proposed classification that is based on two major types of the cyber crime, namely computer-assisted and computer-focused. The computer-assisted cybercrimes are these which use computer as supporting tool and where the target is not to be directly connected with the cyberspace (e.g. harassment). The computer-focused category of crimes includes these incidents that are almost entirely technical, associated with ICT systems and not (or weakly) connected to other sectors.

Similar dichotomized categorisation (as by Furnell) has been proposed by Gordon and Ford [14]. Authors divided cyber terrorism into two distinct classes, namely: (i) Type I Cybercrime, which is mostly technological in nature, (ii) Type II Cybercrime, which has a more pronounced human element.

Different classification is proposed in [15]. It is mainly focused on subject of criminal activity and defines following main categories, namely: against individual, against property, against organization, against society.

In opposite Walden [16] has postulated that there are five possible schemas of classification that overlap but are different in their perspective. These are: technology-based, motivation-based, outcome-based, communication-based and information-based crimes.

According to [17] motivation-based classification schema provides more holistic perspective on the topic cybercrime. The proposed motivational model is composed of five major components: people, motivation, perpetration technology, security barrier and the target. The people in the model refer either to offenders or criminals. When individuals are exposed to a certain type of the factors they may become motivated to carry out particular behaviour and commit a crime. The motivation component refers to certain factors like unemployment, low median income, poverty, or social status that push the individual to carry out a cyber crime. The perpetration technology refers to technology used as a tool to commit a crime, while security barrier indicates components (firewalls, anti-virus software, etc.) that need to be comprised in order for crime attempt to be successful. The last component of the model indicated as Target refers to the people or organization that are being targeted by a criminal.

One of the approaches intending to comprehend cyber security aspects of critical infrastructures have been attempted by the European Union-sponsored project named Vital Infrastructure Threats and Assurance (VITA) [18]. One of the

outcomes of the project was a generic threat taxonomy for Critical Infrastructures (CIs). It categorises such aspects as threat cause, human intent, threat, etc. It is emphasised by authors [19] of the taxonomy that terror, sabotage or activism are not threats but motivations.

In [20] authors adapted and extended the VITA threat taxonomy for Smart Grids. While identifying threats authors have addressed both the information and infrastructure dimension. Authors particularly wanted to identify how Smart Grid hardware may influence the resilience and reliability of energy grids.

Recently, the taxonomy of the cyber crime and cyber terrorism was discussed in [1].

4 CIP Cyber-Physical Security Life-Cycle Models

A wide spectrum of services provided by intelligent critical infrastructures (e.g. Smart Grids) heavily depend on Cyber-Physical Systems (CPS) that are able to monitor, share and manage information. On the other hand, an increasing number of cyber attacks and security breaches are part of rapidly expanding cyber threat, which in many cases has form of cyber terrorism.

The cyber-physical security can be analysed from classical crisis management point of view. In fact, most of incident management processes in the cyber domain follows the ITIL model that is depicted in Fig. 2. It focuses on incidents detection, diagnosis (e.g. identification of exploits that attacker exploited), repairmen (e.g. elimination of the software vulnerability that attacker exploited), recovery and restoration (e.g. to normal business operation status).

However, this type of model may not properly show the iterative nature of continuous improvement that usually are implemented after the crisis as an element of lessons learnt. Therefore, the model of cyber security life-cycle would be that one which is intended to define how to prevent, detect, respond to and recover from cyber crisis, and finally to avoid reoccurrence. Thus, we can define Cyber Attack Timeline, illustrated in Fig. 3, which is constituted of the following three phases:

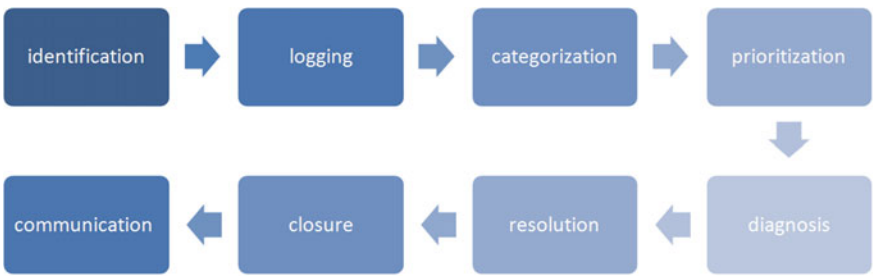


Fig. 2 Incident management according to ITIL standard [35]

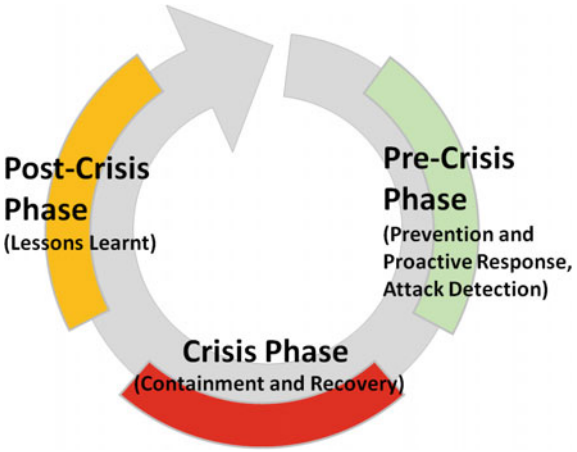


Fig. 3 Cyber crisis management cycle

- A Pre-Crisis (Steady State) phase in which organization aims at providing all services as usual while increasing the preparedness to an critical event. For this phase it is important to have risk management process that will allow the organization for risk anticipation and proactive response.
- A Crisis phase in which a threat has to be maintained and system recovered. It is an emergency case in which it is necessary to change the approach so that threats can be quickly removed and their effects mitigated.
- A Post Crisis phase during which the "lesson learned" as a result of the Crisis phase needs to feedback the whole process in order to reduce its impact in the future.

In this section, we further elaborate on different aspects related to cyber security of CPS systems that is embraced into crisis management phases namely: prevention, detection, containment, and post-incident.

4.1 Pre-crisis Phase

4.1.1 Prevention and Proactive Response

The cyber security prevention is an important aspect when it comes to cyber-physical systems and its impact on critical infrastructures. It requires some amount of the resources to be allocated, however, it is better than often costly recovery (or in worst case no recovery at all). As the value and importance of prevention is at least well acknowledged in the communities, it is still in many cases perceived as product that can be purchased and deployed in an organisation. In fact, the prevention is long-lasting and continuous process reaching far beyond technical problems embracing organisational, regulatory, and human aspects.

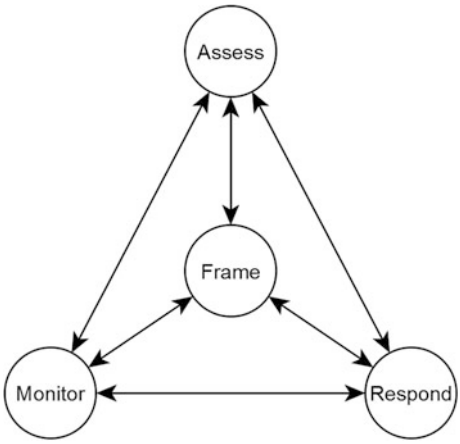


Fig. 4 Risk management—information and communication flows (NIST SP 800-39)

Particularly, the cyber attack prevention requires (within the organisation) well established roles that will be responsible for containing the cyber attack and its causes. This implies that an organisation should define detailed cyber incident response plan that will describe how an incident should be reported, investigated and responded (Fig. 4). Moreover, when the cyber incident involves personal information, it implies various data privacy and security laws that may have different shape in different countries.

As mentioned in [21], it is very important for Critical Infrastructures operators to identify the risks posed by the communication networks and existence of dependencies with third party systems. This is even more important form wider perspective, because such risk anticipation can prevent the possibility of cascading failures causing catastrophic system damages.

The risk management cycle is a comprehensive process (Fig. 2) that requires organizations to:

- frame the risk (i.e., establish the context for risk-based decisions),
- assess the risk,
- respond to the risk once determined,
- monitor the risk.

Usually this requires effective communication and an iterative feedback loop, that will facilitate continuous improvement in the risk-related activities.

As it is suggested by ENISA [22], a good practice for well-suited prevention mechanisms is to subscribe to relevant information sources that would give up-to-date overview of current cyber threats and incidents reported. ENISA also stresses the importance of information sharing.

More local (service based) approach to risk modelling has been proposed by OWASP [23]. The approach follows the idea of decomposition of complex system to smaller components (see Fig. 5 Threat Risk Modelling proposed by OWASP). It is important to stress the fact that all key players (e.g. security officers, employees)

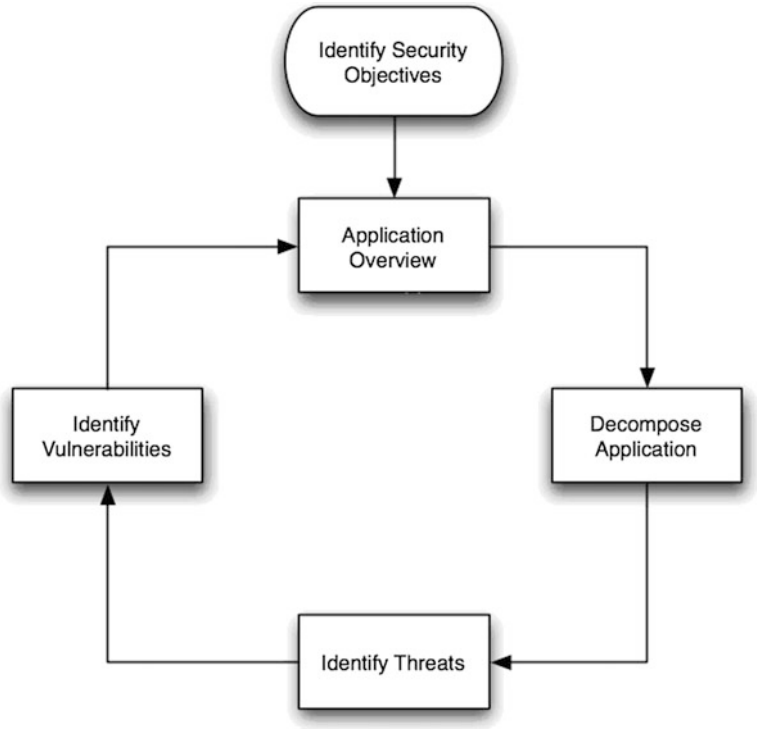


Fig. 5 Threat risk modelling proposed by OWASP [23]

need to understand the security objectives. Therefore, usually the complex system is broken down into objectives such us: reputation, availability, financial, etc. Other security objectives may be enforced by the law (financial or privacy laws), adapted standards (e.g. ISO).

The key element of this risk assessment methodology is the possible threats identification. Microsoft has suggested two different approaches to identify those threats. One is a threat graph (see Fig. 6), as shown in Fig. 2, and the other is a structured list.

4.1.2 Threat Detection

The capability of early detection of cyber threats is a very important element for good cyber crisis preparedness. Probably, one of the most classic way to categorise the cyber attack detection technique is to assign them into one of the following groups, namely: signature-based, anomaly-based or hybrid (Fig. 7).

Each of this class of algorithms has their drawbacks and advantages, and different approaches to identify attacks. Some of the methods have also different

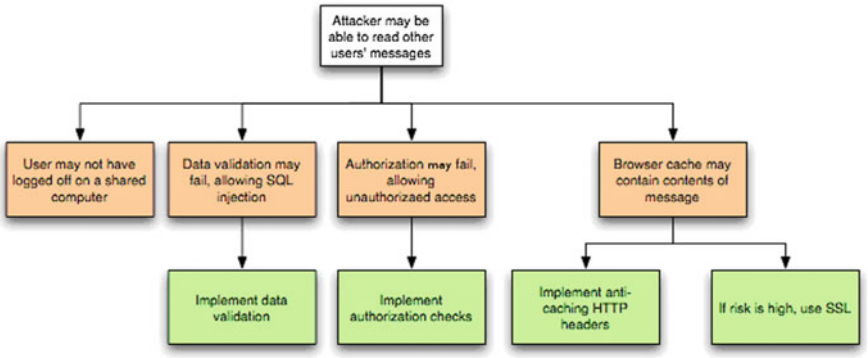


Fig. 6 Threats identification [23]

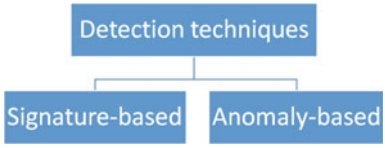


Fig. 7 Attack detection techniques classification

methods for data aggregation (e.g. host-based or network-based) and traffic properties description (e.g. packet-based analysis or aggregated connections flows). All the above mentioned aspects are dissuaded in the consecutive subsections.

The Signature-based category of cyber attacks detection typically include Intrusion Prevention and Detection Systems (IDS and IPS) which use predefined set of patters (or rules) in order to identify an attack. The patterns (or rules) are typically matched against a content of a packet (e.g. TCP/UDP packet header or payload). Commonly IPS and IDS are designed to increase the security level of a computer network trough detection (in case of IDS) and detection and blocking (in case of IPS) of network attacks.

Commonly the patterns an attack for IPS and IDS software are provided by experts form a cyber community. Typically, for a deterministic attacks it is fairly easy to develop patterns that will clearly identify given attack. It often happens when given malicious software (e.g. worm) uses the same protocol to communicate trough network with command and control centre or other instance of such software. However, the problem of developing new signatures becomes more complicated when it comes to a polymorphic worms or viruses. Such software commonly modifies and obfuscates its code (without changing the internal algorithms) in order to be less predictive and easy to detect.

4.2 Crisis Phase

In this phase risk management is not important, because it gives priority to incident management in order to solve crisis and mitigate threats by adopting proper countermeasures. However, it is worth mentioning that the emergency and contingency procedures adopted during a Crisis Phase are developed during the Pre-Crisis phase. In other words, during the Crisis phase it is not only important to have an overall situational awareness picture, but also to have a strategy to recover form crisis in the most efficient way possible. There are different models for cyber incidents handling. For instance, ENISA defines (see Fig. 8) formal manner starting from incident reporting, going through analysis and recovery, and concluding with post-analysis followed by improvements proposal. This model of cyber crisis response is widely adapted by Emergency Response Teams (CERTs). According to definition provided by ENICS [24] CERTs are the key institutions that are obliged to receive, inform and respond to cyber security incidents. At the same time, they act as educational entities in order to raise the cyber-related awareness and provide primary security service for government and citizens. Every single country that is connected to the Internet should have capabilities to respond to cyber-related security incidents. Nevertheless, not every country has such capabilities. One of the

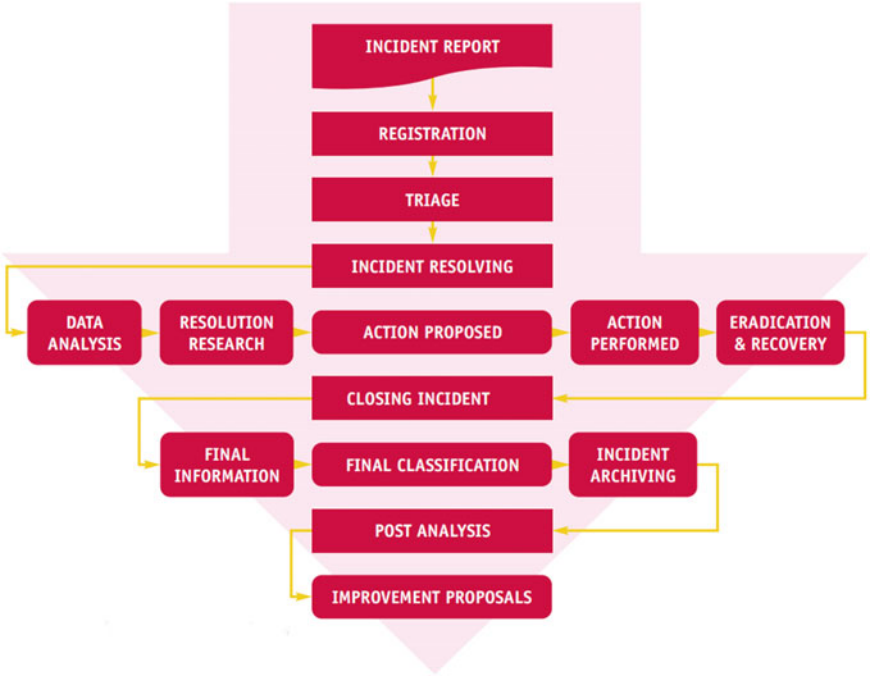


Fig. 8 ENISA incident handling model [22]

earliest CERT teams focused on critical infrastructures was the US ICS-CERT (Industrial Control Systems Cyber Emergency Response Team) that was established in 2009 [25]. This institution aims at reducing the impact of cyber attacks. In order to achieve this goal ICS-CERT takes preventative actions such as vulnerability monitoring and reporting (each year ICS-CERT releases annual reports in order to spread the information about the security incidents).

However, before the actual incident handling will take place, usually the incident is verified and pre-classified, in order to assess its significance, severity and time constrains required to resolve it. This activity is named triage and refers to situation in which there are limited resources and the decision maker has to decide on the priorities of actions relying on the severity of the particular cases.

An important thing, which is not directly reflected by the incident handling model, is fact that CERTs also collaborate with other Computer Emergency Response Teams that are part of international or private sector institutions. This cooperation allows the CERTs to share the information about control systems-related security incidents and mitigation measures.

4.3 Post-crisis Phase

The post crisis phase is the phase in which threat has been eliminated and system has been repaired, thus allowing the restoration of provided services and return to usual business activities.

As recent cyber incidents show, it is important for the Critical Infrastructure operators to have employees that would be educated and skilled in cyber security aspects. The post-crisis phase is important for an organisation to draw some conclusion after the crisis and use this time as an opportunity to increase the number of cyber security professionals at various levels of skill and competence, as well as to upgrade the competence levels of the already hired staff.

In fact, learning from previous experiences is a continuous process for the organisation. According to the terminology adapted in [26] this problem can be decomposed into:

- acquiring experience,
- gathering and analysing experience,
- applying experience.

Obviously, in order to address all of above mentioned aspects, it is necessary to have resources allowing for relevant data gathering and analysis. In many cases, dedicated tools facilitating the end-user with such functionalities are used. Particularly, in the post-crisis phase it is necessary to collect the lessons learnt and analyse the overall crisis scenario from wider perspective in order to identify root cause of the crisis and procedural pitfalls that may have been identified.

In particular, a new risk analysis must be performed in order to evaluate if the previously defined security controls are still effective and to estimate whether risk levels have been changed.

5 Modelling Cyber Security Aspects

There are different approaches to model cyber security aspects. Depending on the goal of the modelling process one can divide these as problem of modelling the (Fig. 9):

- Network,
- Risk,
- Cyber Attack,
- System Behaviour.

5.1 Network Modelling

As for the Network modelling, one can use different network simulation tools (e.g. NS3, NS2, OPNET, NetSim) to analyse selected impacts of cyber attacks on modelled network. For instance, in [27] authors used NS2 simulator to predict the impact of malware propagation, Denial of Service and Man In The Middle attacks on SCADA systems. The authors measure the impact among others in terms of loss of control, Quality of Service (QoS), and number of dropped packets.

Different tools suits allow the user to model different aspects of telecommunication network with a varying granularity using different modelling techniques. In the NS3, the topology and the configuration of the simulation are provided either in *.py (python) or in *.cc (c/c++) files. Commonly, these files contain the following information:

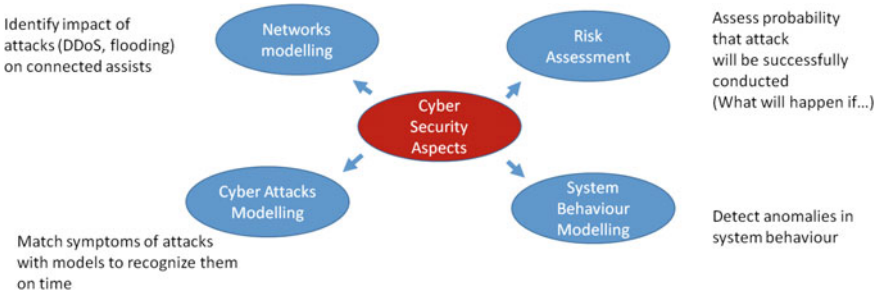


Fig. 9 Different approaches to model cyber aspects

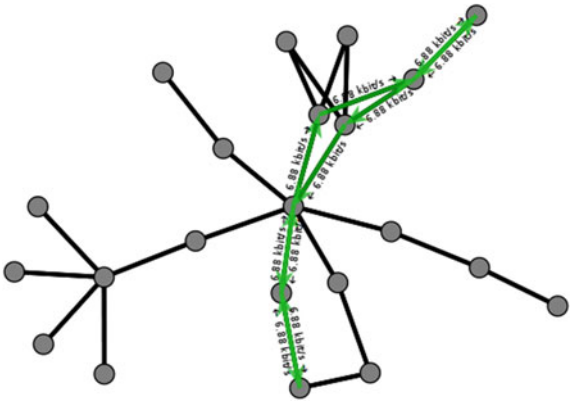


Fig. 10 Example of network topology visualized with PyViz (NS3)

- Nodes definition (names, types, positions, etc.)
- Communication links definition (data rates and delays)
- Topology definition
- IP stack installation
- IP addresses assignment
- Routing definition
- Configuration of the application layer.

In NS3 the term node is used to name an abstract device connected to a network such as end-users hosts, end-systems, routers, switches, hubs etc. Since NS3 does not focus on Internet technologies only, it is the responsibility of simulation creator to define nodes properly by adding applications, protocols stack, etc. In NS3 the concept of application is defined as an element that runs the simulation. It is the basic abstraction of a user program, which generates some network traffic. The NS3 allows the user to use additional tools to visualise simulation at a runtime (see PyViz in Fig. 10) and to prototype the network topology with GUI-enabled software.

5.2 Cyber Risk Assessment

The goal of the tools and methods used for the modelling the cyber risk is similar to the previous approach, however the approach is substantially different. For instance, the aim of tools like Haruspex [28], is to evaluate the probability that an adversaries can implement successful cyber attack against a system. Haruspex implements the simulation as model comprising of threat agents and the attacks they convey. The system is modelled as a set of components interacting through channels. As a final result, the tool collects relevant statistical data from the simulations.

Similar approach to probability-based risk evaluation is presented in [29]. The authors have adapted an ontology to model the system, its key components and interaction between them. Main concepts, which compose main classes of proposed

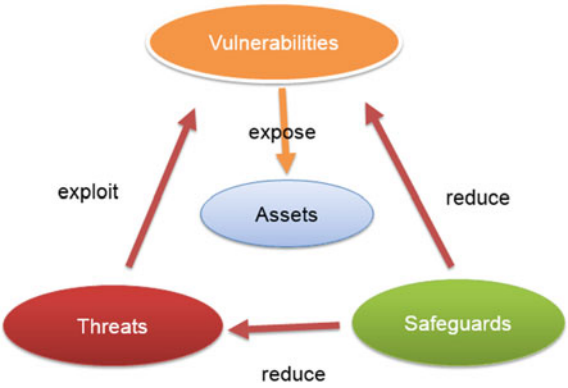


Fig. 11 High-level overview of key classes in the ontology

ontology (see Fig. 11) are Assets (anything that has value to the organization), Vulnerabilities (include weaknesses of an asset or group of assets which can be exploited by threats), Threats (potential cause of an unwanted incident which may result in harm to a system or organization), Safeguards (practices, procedures or mechanisms that reduce vulnerabilities).

As argued by the authors, the ontology-based data models allows for addressing the complexity, diversity, and sparsity of dependencies. An example of instantiated ontology classes is shown in Fig. 12.

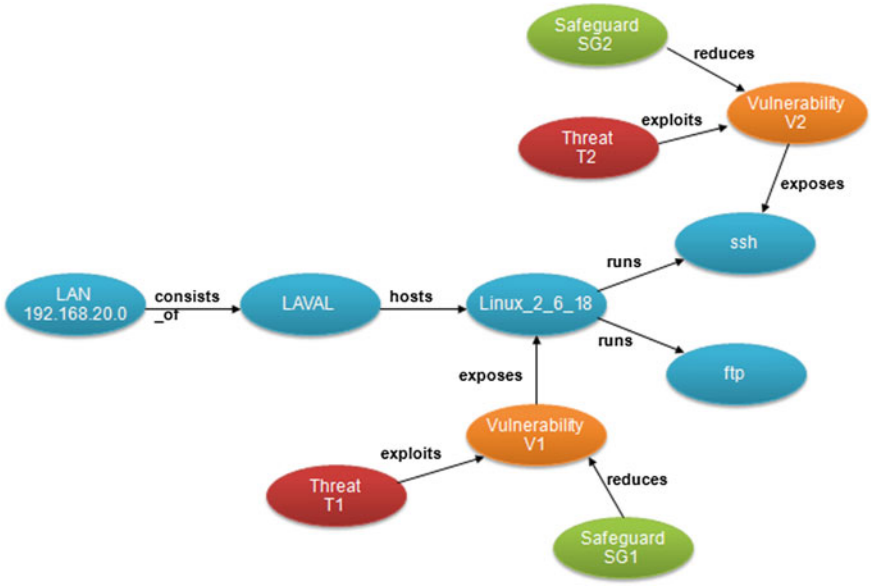


Fig. 12 Ontology-based data model describing elements and dependencies between elements

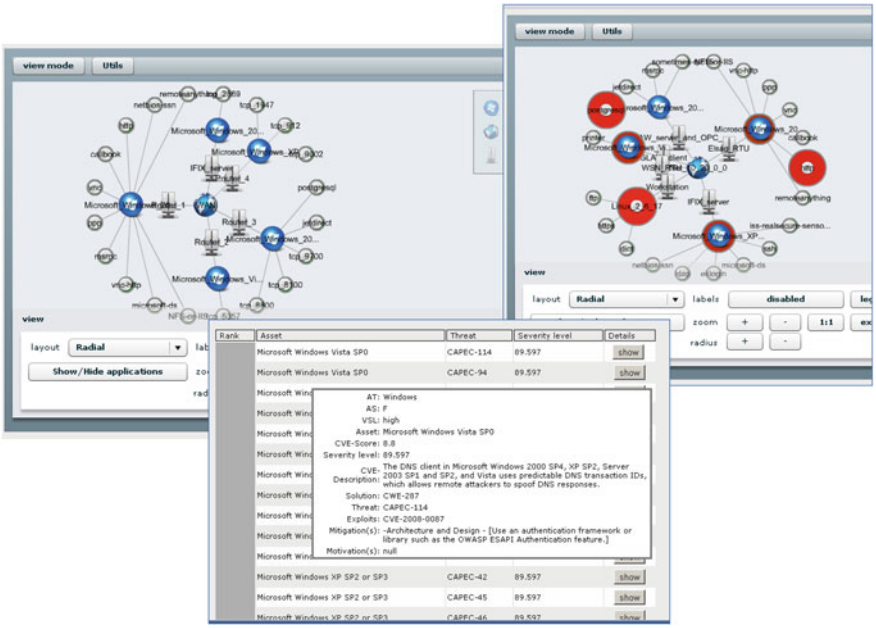


Fig. 13 Example of analysis conveyed by DAT tool [29]

The results of the analysis conveyed with this tool is an interactive security report (see Fig. 13). It allows the operator to go through the list of identified threats and get the detailed description accompanied with security counter measure that is likely to eliminate (or decrease) given risk.

5.3 System Behaviour and Attacks Modelling

The underlying motivation for system and attack modelling is the evolvement of tools and techniques in the area of artificial intelligence, data mining, and classification. Those techniques allow for automated data analysis, novelty and anomaly detection without extensive understanding of the underlying data content. The anomaly-based methods for a cyber attacks detection build a model that is intended to describe normal and abnormal behaviour of network traffic.

The approach to adopt these techniques is in many cases similar. Firstly, sensors collecting relevant data are deployed across network. Typically, these data require further processing in order to extract relevant information (average value of measured physical property or number of packet transmitted, see Fig. 14).

Commonly such methods uses two types of algorithms from machine learning theory, namely unsupervised and supervised approach.

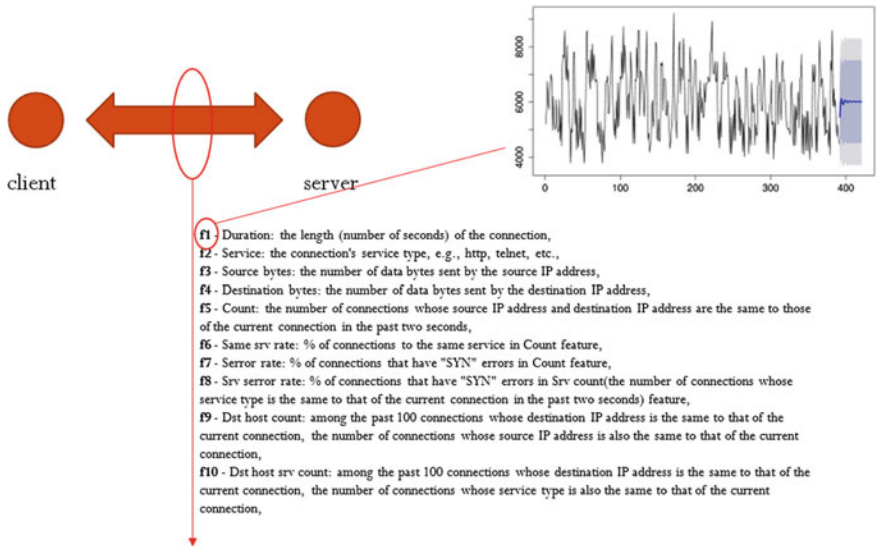


Fig. 14 A conceptual overview of on-line analysis

For unsupervised learning commonly clustering approaches are used that usually adapt algorithms like k-means, fuzzy c-means, QT, and SVM. The clustered network traffic established using mentioned approaches commonly requires decision whenever given cluster should be indicated as a malicious or not. Pure unsupervised algorithms uses a majority rule telling that only the biggest clusters are considered normal. That means that network events that happens frequently have no symptoms of an attack. In practice, it is a human role to indicate which cluster should be considered as the abnormal one.

The supervised machine learning techniques requires at least one phase of learning in order to establish the model traffic. The learning is typically off-line one and is conducted on specially prepared (cleaned) traffic traces. One of the exemplar approaches to supervised machine learning for cyber attack detection use auto regression stochastic process (AR). In literature there are also methods using Kalman filters. Recently, more gaining in popularity are solutions adapting SVM, neural networks, and ID3-established decision trees.

6 Ongoing Efforts

6.1 H2020 Work Program View on CPS Aspects

The research topics defined for the security call in Horizon 2020 programme reflect the need for securing Critical Infrastructures—both physically as well as in digital

domain, preventing them from cyber-attacks. For example, the topic CIP-01-2016-2017 entitled "Prevention, detection, response and mitigation of the combination of physical and cyber threats to the critical infrastructure of Europe" addresses aspects of cyber and physical security convergence to protect installations of the critical infrastructure of Europe. The challenge related to such protection is not only addressing separately physical threats to CI (such as bombing and other terrorists acts and natural-born threats as seismic activities or floods) and cyber threats, but establishment of security management paradigms that include the combinations of both group of threats, analysis of their interconnections and cascading effects resulting from cyber or physical damages. Also, it is expected that research initiatives acting under this topic will pursuit solutions related to sharing information with the public in the region of affected installations, and the protection of rescue teams, security teams and monitoring teams. The main expected results of the research in short- and medium-term perspectives include analysis of physical/cyber detection technologies and risk scenarios in the context of a specific critical infrastructure, analysis of physical-cyber vulnerabilities of a specific critical infrastructure, development of tools, concepts, and technologies for combating both physical and cyber threats to a specific critical infrastructure. These tools should be innovative, integrated, and dedicated to prevent, detect, respond and mitigate physical and cyber threats and enabling monitoring of the environment, communication with the inhabitants in the vicinity of the critical infrastructure. In long-term perspective, achievement of convergence of safety and security standards, and the establishment of relevant certification mechanisms are expected in this area.

Another example of topic in which the importance cyber-physical security is emphasized is DS-01-2016: "Assurance and Certification for Trustworthy and Secure ICT systems, services and components". In particular, specific nature of CPS systems (that smart meters are highly connected to) as evolving, complex and dynamically changing environment makes critical security-related decisions very challenging and demanding a technology-based support.

Moreover, topics from past security call (H2020 WP2014-15) also addressed problems of cyber-physical security convergence. One of examples was DRS-12-2015 topic, entitled "Critical Infrastructure smart grid protection and resilience under smart meters threats", under which physical safety (threat of undesired physical access to smart meters) was examined alongside other cyber threats.

6.2 Security Standards for Critical Infrastructures

In this section we provide the short overview of wide spectrum of different standards that address the cyber (as well as physical) security aspects of critical infrastructures.

The ISA99 committee addresses the cyber security of industrial automation and control systems by its ISA/IEC-62443 series of standards. The scope of the ISA99

standards is very broad, i.e. the committee does not limit application of its standards to the specific type of plants, facilities or systems. Manufacturing and control systems to which the ISA/IEC-62443 can be applicable include hardware and software systems such as DCS, PLC, SCADA, networked electronic sensing, monitoring and diagnostic systems as well as associated interfaces used to provide control, security, and continuity of industrial processes. In the ISA/IEC-62443 series of standards physical security is not directly addressed, despite the fact that physical security highly impacts the integrity of any control system environment [30].

The NERC (North American Electric Reliability Corporation) CIP plan is a set of requirements designed to secure the assets required for operating North America's bulk electric system. This set includes 9 security standards and 45 requirements and addresses security of electric systems and the protection of the critical cyber assets operating within these systems. Cyber security training, management and crisis recovery are also included. Physical security of Critical electric systems is covered by the CIP-006-1: Physical Security of Critical Cyber Assets sub-standard [31, 32].

The IEC 62210 technical report on "Data and Communications Security" can be applied to supervision, control, metering and protection systems in electrical utilities. The report covers a broad range of security related aspects such as definitions, prioritization of threats, consequence analysis, attacks, policies and "Common Criteria" protection profile. Communication protocols used within and between systems, secure use of the systems and access to them are also discussed. Consequence analysis was adopted in the report as the security methodology for prioritization of assets and threats to the security of the some industrial protocols e.g. TC 57 protocol used for power systems management and exchange of associated information. However, as it is stated in the report, the document does not include recommendations or criteria development related to physical security of critical systems [33]. In addition, IEC 62351 is a series of technical specifications covering aspects of information security for power system control operations. Selected aspects that are discussed in IEC 62351 are authentication of data exchange (digital signatures, certificates), security of TCP/IP (e.g. encryption), networks and systems security management and key management.

Also the IEEE 1402 standard applies to the power distribution and critical energy infrastructures protection, however in a contrary to above described IEC documents, this standard addresses aspects of physical security, especially in a context of unauthorized access to electric power substations. The document describes and guides a variety of methods to prevent such substations from human intrusion [34].

7 Conclusions

In this paper we have described various cyber security aspects related to the cyber-physical systems and critical infrastructures. We have described current challenges related to the technical aspects as well as the European vision on that

matters. As we currently observe, due to the evolution of Internet and the wide adoption of the Internet of Things concept, we may expect that in the near future the cyber security of cyber-physical systems will become of even higher importance. As gradually increasing number of elements and aspects (smart devices, homes, cars, etc.) of our lives becomes connected to the Internet, it gives new opportunities and motivations for the cyber criminals to research and to exploit technological vulnerabilities in order to gain economical profits. Those attempts cannot be successful with regards to critical infrastructures and homeland security.

Therefore new technological and organizational solutions are needed for cyber physical systems protection. There are also many urgent questions and aspects to be addressed by nations and companies, such as if the standards and guidelines for cyber security should be obligatory and mandatory (which also involved controlling organizations and possible penalties), or if those should rather be voluntary. Moreover, the minimal security standards have to be defined. Another difficulty is to find the right balance for the appropriate level of details of recommendations and standards. Should those be rather general, universal and high level (for further customization for each organization), or should those be as detailed as possible mentioning particular technologies and solutions to be applied. At the nations level, the decision should be also made who (which organizations) should issue such standards and guidelines. Should those be sectorial organizations (e.g. for standards for energy, healthcare, financial sector etc.) or rather ministries covering wider range of applications?

However, the most crucial aspects now for protecting critical infrastructures is the awareness building. Without the understanding and awareness of all the actors (private CI owners, governments, managers, employees at all levels etc.) our critical infrastructures will be still endangered by the cyber and physical attacks.

Acknowledgement and Disclaimer This chapter was derived from the FP7 project CIPRNet, which has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no. 312450. The contents of this chapter do not necessarily reflect the official opinion of the European Union. Responsibility for the information and views expressed herein lies entirely with the author(s).

The work is also funded by Polish National Centre for Research and Development (NCBiR) from funds for science in the years 2013–2016 allocated for the international projects.

References

1. Lemos R (2015) Internet of things security check: how 3 smart devices can be dumb about the risks. PCWorld. IDG Consumer
2. Akhgar B, Choraś M, Brewster B, Bosco F, Vermeersch E, Puchalski D, Wells D (2016) Consolidated taxonomy and research roadmap for cybercrime and cyberterrorism. In: Akhgar B, Brewster B (eds) Combatting cybercrime and cyberterrorism—challenges, trends and priorities. Advanced sciences and technologies for security applications. Springer, Switzerland, pp 295–321
3. Stuxnet. http://security.blogs.cnn.com/category/middle-east/iran/stuxnet/

4. Stuxnet computer worm. http://www.cbsnews.com/8301-18560_162-57460009/stuxnet-computer-worm-opens-new-era-of-warfare
5. Hackers hijacking water treatment plant controls shows how easily civilians could be poisoned. http://www.ibtimes.co.uk/hackers-hijacked-chemical-controls-water-treatment-plant-utility-company-was-using-1988-server-1551266
6. Attack targeting Health Care. http://www.ucdmc.ucdavis.edu/welcome/features/2010-2011/08/20100811_cyberterrorism.html
7. Cyber attack on Health Care institution. http://www.bakersfieldcalifornian.com/local/x534570019/Kern-Medical-Center-battling-virus
8. Financial institutions on high alert for major cyber attack. http://www.computerweekly.com/news/4500272926/Financial-institutions-on-high-alert-for-major-cyber-attack
9. How cyber criminals targeted almost $1bn in Bangladesh Bank heist. http://www.ft.com/cms/s/0/39ec1e84-ec45-11e5-bb79-2303682345c8.html
10. Emerging Cyber Threats Report (2016) Georgia Institute of Technology
11. Choraś M, Kozik R, Churchill A, Yautsiukhin A (2016) Are we doing all the right things to counter cybercrime? In: Akhgar B, Brewster B (eds) Combatting cybercrime and cyberterrorism—challenges, trends and priorities. Advanced sciences and technologies for security applications. Springer, Switzerland, pp 279–294
12. Furnell SM (2001) The problem of categorising cybercrime and cybercriminals. In: 2nd Australian information warfare and security conference 2001
13. Audit Commission (1998) Ghost in the machine: an analysis of IT fraud and abuse. Audit Commission Publications, London
14. Gordon S, Ford R (2006) On the definition and classification of cybercrime. J Comput Virol 2:13–20
15. Report Cyber Crime homepage. Cyber crime classification. http://www.reportcybercrime.com/classification.php
16. Walden I (2007) Computer crimes and computer investigations. Oxford University Press, USA. Wall DS (ed) (2001) Crime and the internet. Routledge, London (ISBN 0415244293)
17. Ngafeeson M (2010) Cybercrime classification: a motivational model. College of Business Administration, The University of Texas-Pan American. 1201 West University
18. Directorate General for Enterprise and Industry European Commission (2009) VITA—Vital infrastructure threats and assurance
19. Luiijf HAM, Nieuwenhuijs AH (2008) Extensible threat taxonomy for critical infrastructures. Int J Crit Infrastruct 4(4):409–417
20. Luiijf HAM (2012) Threat analysis: work package 1.2—expert group on the security and resilience of communication networks and information systems for smart grids, report, 2012
21. Buldyrev SV et al (2010) Catastrophic cascade of failures in interdependent networks. Nature
22. ENISA (2011) New guide on cyber security incident management to support the fight against cyber attacks
23. Threat Risk Modeling. https://www.owasp.org/index.php/Threat_Risk_Modeling
24. CERT. ENISA homepage. http://www.enisa.europa.eu/activities/cert
25. ICS-CERT. http://ics-cert.us-cert.gov/
26. LIMA2 tool. http://www.proceed.itti.com.pl/?p=218&lang=en
27. Ciancamerla E, Minichino M, Palmieri S (2013) Modeling cyber attacks on a critical infrastructure scenario. In: 2013 fourth international conference on information, intelligence, systems and applications (IISA), Piraeus, pp 1–6
28. Haruspex-Simulation-driven Risk Analysis for Complex Systems. http://www.isaca.org/Journal/archives/2012/Volume-3/Pages/Haruspex-Simulation-driven-Risk-Analysis-for-Complex-Systems.aspx
29. Choraś M, Flizikowski A, Kozik R, Renk R, Holubowicz W (2009) Ontology-based reasoning combined with inference engine for SCADA-ICT interdependencies, vulnerabilities and threats analysis. In: Pre-proceedings of 4th international workshop on critical information infrastructures security, CRITIS'09, Bonn, Germany. Fraunhofer IAIS, pp 203–214
30. https://www.isa.org/isa99/

31. http://searchcompliance.techtarget.com/definition/NERC-CIP-critical-infrastructure-protection
32. http://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx
33. IEC TR 62210 (2003) Power system control and associated communications—data and communication security. IEC technical report
34. IEC TS 62351 (2007) Power systems management and associated information exchange—data and communications security. IEC technical specification
35. ITIL Incident Management. http://www.bmc.com/guides/itil-incident-management.html

Chapter 8
Verification and Validation for CIPRNet

Jeroen Voogd

Abstract In this chapter it is shown that if an appreciable risk is present in the use of Modelling and Simulation (M&S), Verification and Validation (V&V) should be employed to manage and mitigate that risk. The use of M&S in the domain of critical infrastructure (CI) will always be accompanied by such a risk. It is important that a structured approach to V&V is used in order to be more effective and more efficient than just testing without a clear plan. The Generic Methodology for V&V (GM-VV) is a recommended practise in the international M&S community and adopted by large organisations such as NATO. The GM-VV has a number of concepts that allow for a structured approach to V&V. A structured approach to V&V such as the GM-VV leads to a set of handles that allow the best choices for V&V techniques to employ. The choice for a specific technique is dependent on a number of factors such as the needed certainty, the expected residual uncertainty of the proposed technique and its requirements in terms of costs, real-world knowledge, etc. This chapter is divided in 4 parts. The first part has the take away message "You have to do Verification and Validation because there is risk involved", the second "You have to do it in a structured way if you want to do it more effective and more efficient" and the third "You have to choose the appropriate Verification and Validation technique to balance risk, effectiveness and efficiency." In the last part some conclusions are drawn.

1 Do V&V If There Is Risk Involved

In this section we first briefly explain what Modelling and Simulation (M&S) are. It will be made clear that if the M&S results are applied in the real world, M&S Use Risk has to be considered. To manage this risk it is required to have insight into the

J. Voogd (✉)
Modelling, Simulation and Gaming, TNO, Oude Waalsdorperweg 63, PO Box 96864, 2597 AK The Hague, The Netherlands
e-mail: jeroen.voogd@tno.nl

R. Setola et al. (eds.), *Managing the Complexity of Critical Infrastructures*,
Studies in Systems, Decision and Control 90,
DOI 10.1007/978-3-319-51043-9_8

quality and associated risk of the M&S system over its entire life cycle. Verification and Validation are the two processes to obtain this insight. These processes are also briefly explained.

1.1 Modelling and Simulation

Modelling and simulation start—as all system engineering projects do—with a purpose. Then the modelling starts. A possible definition of a model is that it is an abstract representation or specification of a system. A model can represent a system that exists in our material world but can also represent not yet existing systems or combinations thereof. That part of (the imagined) reality that the model is supposed to represent is called the *simuland*. Then further abstractions are applied to the simuland in order to make the model suited for its purpose. Abstraction in this context is a process in which a relative sparse set of relevant (sub)systems, relationships and their inherent qualities are extracted or separated from the more complex (imagined) reality (Fig. 1).

In a simulation the model is used to replicate the simuland behaviour. Thus a simulation is a method, software framework or system to implement and evaluate a model over time i.e., it is a system in which a model is made to execute and is exercised. This model in its executable form is called the M&S system.

The M&S system is provided with input and its output is used within a certain context provided by a frame such as shown in Fig. 2 which is called the Simulation Frame. The model that is executed in the simulation is controlled and observed by means of its ports (ellipses in Fig. 2). Through these ports simulation data, stimuli or settings are entered into the model and simulation output leaving the executed model is observed. During the simulation the model behaves according to a dynamics that represent the state change and behavioural properties of the simuland. The notion of time, behavioural representation and frame are fundamental characteristics of a simulation.

To properly replicate the simuland for the intended use, the model is configured, controlled and stimulated by the Simulation Frame by means of input trajectories,

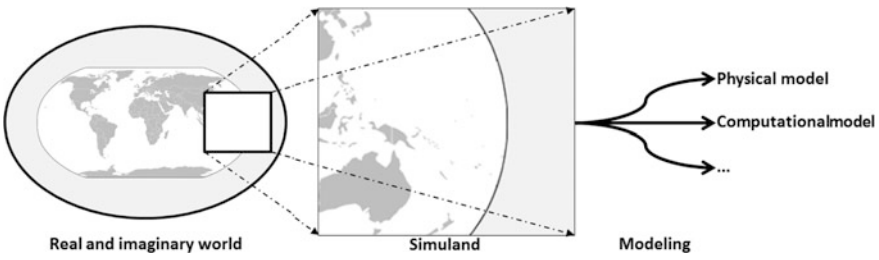


Fig. 1 Modelling is taking abstractions

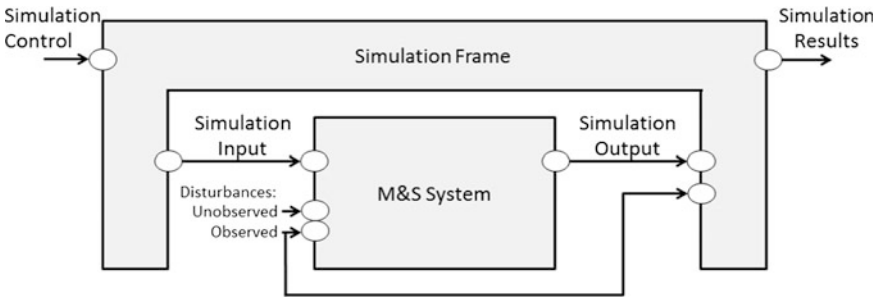


Fig. 2 Relation between simulation frame and the M&S system

scenario's, parameters, environment variable settings and experimental control settings. Furthermore, environment disturbances coming from connections with live entities may impact the behaviour of the M&S system. During the execution of the model, human input can become part of the displayed behaviour. This can be from trainees, but also from operators such as opponent players to provide stimuli to the trainees or Subject Matter Experts (SMEs) that interfere with the execution of the simulation for some purpose dictated by the Simulation Frame (e.g., keeping the execution within a desired regime).

So, all in all the M&S process consists of cutting away all elements of the real and imaginary world that are not needed for the purpose at hand, then apply various abstraction techniques to make the model suited for use, then the model is executed in order to obtain results (e.g. a trained operator or an optimized CI configuration). These results are then applied in some form or another in the real world.

And that last part is exactly where the risk exists. When the M&S-based solutions to problems are applied in the real world there is a risk that those results are not fully appropriate. There can be a number of causes: the purpose for the M&S endeavour was not what was ultimately needed, maybe the simuland did not contain all needed elements of the real and imaginary world, maybe some abstractions were too large and important details were abstracted away, maybe the implementation and execution of the model or the interpretation of it's results introduced errors.

If the results of M&S are never used in the real world, e.g. if it is used for entertainment purposes or as a hobby, then there is no problem. But for CI this is not the case. The possible sources of errors may for example lead to operators of actual CI taking wrong actions if M&S was used for their training. If it is used for determining the best possible configuration of interconnecting CI, it may result in a system that performs less than desired.

The conclusion is that we need to be sure that the M&S results are fit for purpose before actually applying them to the real world. There are two processes that do exactly that: Verification and Validation. Therefore the take away message of this part is "You have to do Verification and Validation because there is risk involved".

1.2 Verification and Validation

There is no true consensus on the exact definitions of what Verification and Validation (V&V) are. Some definitions are:

Verification. The process of providing evidence justifying the M&S system's correctness [1]. Confirmation, through the provision of objective evidence that specified requirements have been fulfilled [2]. The process of determining that a model or simulation implementation and its associated data accurately represent the developer's conceptual description and specifications [3]. The process of determining the degree that a model, simulation, or data accurately represent its conceptual description and its specifications [4].

Correctness. The extent to which an M&S system implementation conforms to its specifications and is free of design and development errors [1].

Validation. The process of providing evidence justifying the M&S system's validity [1]. Confirmation, through the provision of objective evidence that the requirements for a specific intended use or application have been fulfilled [2]. The process of determining the degree to which a model or simulation and its associated data are an accurate representation of the real-world from the perspective of the intended uses of the model [3]. The process of determining the degree to which a model, simulation, or data is an accurate representation of the real world, from the perspective of the intended purpose of the model, simulation or data [4].

Validity. The property of an M&S system's representation of the simuland to correspond sufficiently enough with the referent for the intended use [1]. The property of a model, simulation or federation of models and simulations representations being complete and correct enough for the intended use [5].

A more intuitive explanation can be seen in Fig. 3. There the blue arrows indicate verification: starting from the specification of the M&S system, a simuland is made, which, after modelling, results in an implementation that can be executed to obtain M&S results. At each step one can check if the transformation has been done correctly and the goal is to show that the M&S system adheres to the specification. In literature one often finds that verification assesses if the M&S is built and used right.

Validation, which is the red arrow in Fig. 3, on the other hand, is making sure that the M&S results produced by the M&S system are fit for the customer's needs

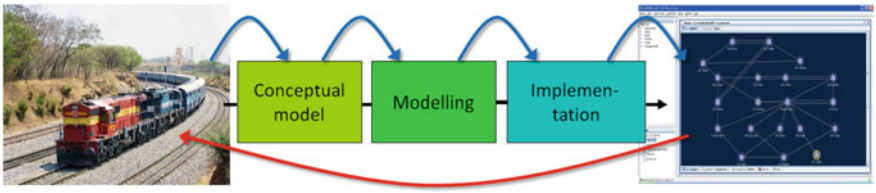


Fig. 3 Verification (*blue arrows*) and Validation (*red arrow*)

in the real world. In literature one often finds that validation assesses if the right M&S is built or procured.

During the execution of V&V it may (and usually will) happen that elements of the M&S System or its use, are found that are not correct or that contribute negatively to the customer's need. Identifying these sources of risk are necessary in order to start managing them. In short: doing V&V provides insight into and advice on the quality of the M&S system over its entire life cycle, and the associated risks.

When studying literature on V&V another term is often found: accreditation. This is, however, a somewhat problematic concept. According to [3] accreditation is "The official certification that a model or simulation and its associated data are acceptable for use for a specific purpose." One problem is that in most countries and for most application domains of M&S there is no official body that can issue such M&S certificates. And besides often the word accreditation is reserved for the official recognition that an organization is allowed to issue certificates. The official certification is called just that: certification (and not accreditation).

In this text the word accreditation or certification is not used. What is assumed is that the result of doing V&V is a body of knowledge on the quality and deficiencies and their associated risks, based on which the customer can decide whether to accept the M&S system or not.

1.3 But How to Do V&V, and How Much?

As described above, for M&S applied to CI it is necessary to identify and manage risk. V&V can be used for that but the question is how should the V&V be approached and how much effort should be spend on it.

The second question is difficult to answer because there is no general answer. Doing V&V can be costly and it should be in balance with the M&S Use Risk involved. Another aspect that has to be considered is the risk tolerance, e.g. in the form of insurance, of the user. What is most important is that the cost spent on the V&V effort should be in balance with the possible costs associated with the risk. The cost of doing V&V should also be significantly less than the possible saving due to risk reduction.

The first question—how to do V&V—is easier to answer. In practice it is often observed that those who develop the simulation also perform the V&V activities. Although they often do a good job, the result does leave something to be desired. After the V&V activities it is not clear anymore which tests were performed and why. The documentation is more often than not a bunch of files on the developer's computer. If after some time things need to be changed in the M&S system and thus some additional V&V activities have to be performed, it is not clear which of the results from the initial V&V activities are still applicable and which tests need to be redone. In short: there is no traceable path from the user's goal to the tests to the results, and no re-usable documentation exists. An unstructured approach to doing V&V may be effective, but often this cannot be shown. It may also be efficient at

first, but again it cannot be shown that the most efficient way of doing V&V tests has been chosen.

So, the question arises if there is a V&V approach that does work well. The first thing to look at is if there are appropriate standards for doing V&V. It turns out that there are a number of V&V approaches for M&S, but these are often domain specific, strongly tied to a specific technology or developer oriented. If that is what is needed, then use them. In general, however, it is not advised to use a developer-oriented approach because the link with the user's goal is not clear. If the V&V effort does not involve a specific domain or technology for which a V&V standard is available, then a more general V&V approach is required.

In order to make sure the V&V effort is effective, the starting point has to be the goal of the user, or to be more precise: the M&S Use Risk associated with the user's goal. From that starting point criteria need to be derived that show what needs to be tested. That derivation and choosing V&V techniques for doing the tests needs to be within the limits of the resources available for the V&V effort, which in practice is always rather limited. The results of the V&V effort need to be documented in such a way that all results can be traced back to the tests and the user's goal, and it should also be such that re-use at a later data is possible. In short: the V&V approach must result in the biggest bang for the buck as well as allow full traceability, otherwise serious questions can be raised about the effectiveness and efficiency of the V&V effort.

The take away message of this section is "You have to do V&V in a structured way if you want to do it more effective and more efficient".

2 Do V&V in a Structured Way to Be More Effective and Efficient

The choice of which V&V method works best in a given situation depends on the individual needs and constraints of an M&S organization, project, application domain or technology. Moreover, V&V usually requires a complex mixture of various activities, methods, tools, techniques and application domain knowledge, which are often tightly coupled with the M&S development process. Therefore, many different approaches to V&V exist that rely on a wide variety of different V&V terms, concepts, products, processes, tools or techniques. In many cases, the resulting proliferation restricts or even works against the transition of V&V results from one M&S organization, project, and technology or application domain to another. Furthermore, history shows that V&V is often more of an afterthought than a built-in part of an M&S development, employment and procurement policy.

The purpose of the Generic Methodology for V&V (GM-VV) is to address these issues by means of providing general applicable guidance for V&V that:

- Facilitates common understanding and communication of V&V within the M&S community.
- Is applicable to any phase of the M&S life-cycle (e.g., development, employment, and reuse).
- Is M&S stakeholders' acceptance decision-making process-oriented.
- Is driven by the M&S stakeholders' needs and M&S use risks tolerances.
- Is scalable to fit any M&S scope, budget, resources and use-risks thresholds.
- Is applicable to a wide variety of M&S technologies and application domains.
- Will result in traceable, reproducible and transparent evidence-based acceptance arguments.
- Can be instantiated on enterprise, project or technical levels alike.
- Facilitates reuse and interoperability of V&V outcomes, tools and techniques.

GM-VV is not aimed to replace the existing V&V approaches, methodologies, standards or policies of M&S organizations, technology and application domains; nor is GM-VV's intent to substitute common enterprise or project management practices prevalent within M&S client or supplier organizations. In addition, GM-VV is not intended to be prescriptive, in that it does not specify a single concrete or unique solution for all V&V applications. Rather, the GM-VV should be tailored to meet the needs of individual V&V applications.

The GM-VV provides a technical framework that focuses on M&S V&V practices. Though interrelated, acceptance decision processes and associated practices such as M&S accreditation and certification are outside the scope of the methodology. GM-VV attains its generic quality from a technical framework that consists of three subparts: the conceptual, implementation and tailoring framework (Fig. 4). This framework is rooted in established international standards and other related practices. The conceptual framework provides the terminology, concepts and principles to facilitate communication and a common understanding and execution of V&V within an M&S context. The implementation framework translates these concepts and principles into a set of generic building blocks to develop consistent V&V solutions for an individual M&S organization, project, and technology or application domain. GM-VV provides a tailoring framework that utilizes these building blocks to develop and cost-efficiently apply such V&V application instances. As such, the GM-VV provides a high-level framework for developing concrete V&V solutions and conducting V&V, into which lower-level practices (e.g., tools, techniques, tasks, acceptability criteria, documentation templates) native to each individual M&S organization, project, technology or application domain can easily be integrated.

Each of the three frameworks will be described in sections below.

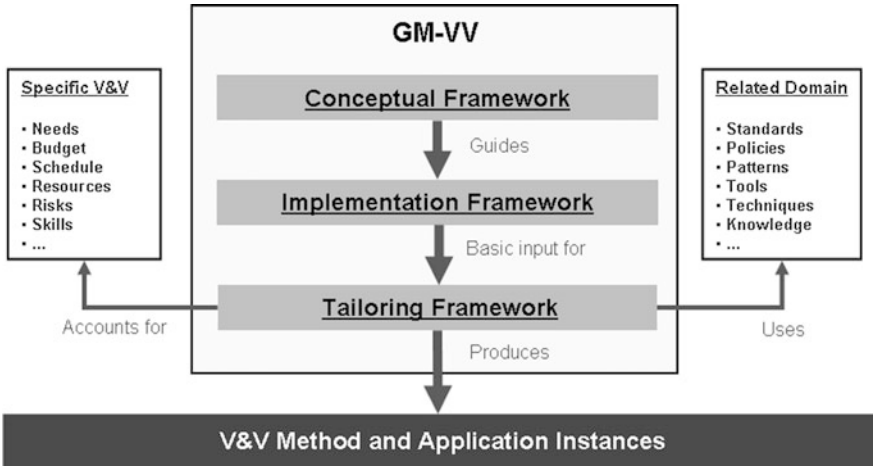


Fig. 4 GM-VV technical framework design and operational use concept

2.1 Conceptual Framework

This section discusses the GM-VV conceptual framework. This framework provides fundamental and general applicable terminology, semantics, concepts and principles for V&V. The purpose of the framework is to facilitate communication, understanding and implementation of V&V across and between different M&S contexts (e.g., organizations, application domains, standards, technologies). The framework is the foundation upon which the GM-VV implementation framework rests.

2.1.1 Links to Systems Engineering

Within the GM-VV, M&S systems are considered to be systems of systems that have a lifecycle and are subject to system engineering practices. Moreover, models and simulations are considered to be part of a larger system in which they are used. From this perspective, M&S is a systems engineering specialization. V&V is an intrinsic part of the systems engineering process [6–9]. Therefore, the GM-VV considers the V&V of M&S as a specialization of systems engineering V&V. Hence, the GM-VV can be integrated with, complement or extend the V&V processes within such existing systems engineering methodologies or standards.

2.1.2 M&S-Based Problem Solving Approach

The basic premise of the GM-VV is that models and simulations are always developed and employed to fulfil the specific needs of their end users (e.g., trainers, analysts, decision makers). Modelling and simulation is thus considered to be a problem solving process that transforms a simple statement of an end user's need into an M&S-based solution for the problem implied in the need. The GM-VV assumes that V&V always takes place within such larger context. This context is abstracted by means of defining four interrelated worlds (Fig. 5). Together, these four worlds define a generic lifecycle and process view of M&S-based problem solving. A view that serves as a common basis, in which V&V for M&S (e.g., concepts, principles, processes, products, techniques) can be understood, developed or applied.

These four worlds can be described as follows:

- **Real World**: The Real World is, as the name suggests, the actual real-life world of which we are part of. It is where the need for some solution arises and where the solution is applied to obtain the desired outcomes. It is also where the real operational and other business risks exist in case the M&S based problem solution is not fit for purpose. Stakeholders from this world may for example be CI facility owners that need well trained operators as well as the general public that wishes to use these facilities and desire a stable service.
- **Problem World**: In the Problem World the needs of the Real World are further examined and solved. For some needs the problem may be training, in which case the Problem World is actually the "Training World", or if the need involves analysis it is the "Analysis World". Here the generic "Problem World" is used. The problem solution may consist of different parts, for example a training program may consist of class room training, simulator based training and live training; an analysis may consist of a literature study, simulation based analysis and expert interviews. In the Problem World the complete problem is solved. Thus the simulation based component (i.e., M&S results) may only be part of the solution.

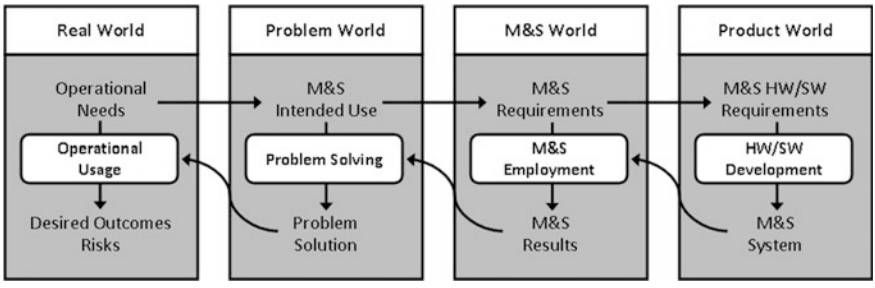


Fig. 5 Four worlds view of M&S based problem solving

Stakeholders from within the Problem World are those parties involved in the complete solution (e.g., organizations) such as education centres and their trainers in case of training, analysts in case of an analysis problem. Stakeholders from the Real World or their experts are typically also involved in the Problem World.

- **M&S World**: In the M&S World the focus is on the M&S based components of the Problem Solution. Here M&S (sub)systems are defined and used. It starts with the specified M&S intended use from the Problem World from which the requirements are derived such as the M&S System components that are needed, which scenarios are to be used and which personnel (trainers, scenario builders, etc.) are needed. After the M&S System becomes available from the "Product World" the execution takes place and the M&S Results are constructed. Stakeholders from within the M&S World are trainers, trainees, analysts or other controllers that control the simulation.
- **Product World**: The Product World takes the M&S requirements from the M&S World and determines the M&S hardware and software requirements. The M&S System is constructed and delivered to the M&S World. Stakeholders within the Product World are those organizations that build and deliver the M&S System such as programmers, model developers, system or software architects and managers of repositories with reusable models.

When the M&S problem solving process described by the four-worlds view is properly executed, the resulting solution should satisfy the originally identified needs with a minimal level of (use) risk in the Real World.

The M&S system, M&S requirements, M&S results and other development artefacts (e.g., conceptual model, software design, code) are thus always directed toward contributing to and satisfying the Real World operational needs. The degree of success of such M&S in satisfying these needs depends on how well they are specified, designed, developed, integrated, tested, used, and supported. These M&S activities require the contribution of individuals or organizations that have a vested interest in the success of the M&S asset, either directly or indirectly. An individual or organization with such interest is referred to in GM-VV as a stakeholder. Stakeholders can play one or more roles in each of the four worlds such as M&S user/sponsor, supplier, project manager, software developer, operator, customer, or subject matter expert (SME). Depending upon their role, stakeholders may hold different responsibilities in the M&S life-cycle processes, activities or tasks.

2.1.3 V&V Problem Solving Approach

Within the four-world context, stakeholders exist who are responsible for making acceptance decisions on the use of M&S. Within the GM-VV, these stakeholders are referred as V&V User/Sponsor. In this context the V&V User/Sponsor could be an M&S User/Sponsor, Accreditation Authority or any other domain specific role

that uses the outcomes of the V&V. V&V Users/Sponsors face the problem of having to make a judgment on the development and suitability of the M&S system or results for an intended use. The key issue here is that it is not possible to demonstrate with absolute certainty that the M&S system or results will meet the Real World needs prior to its actual use. Consequently, there is always a probability that the M&S-based solution is not successful when used (i.e., fails). Such a failure would result in an undesirable impact (i.e., a risk) on the operational environment. Therefore, an M&S system or result is only acceptable to the V&V User/Sponsor if he or she has sufficient confidence that the use of an M&S system or result satisfies the Real World needs without posing unacceptable risks (e.g., costs, liabilities). This M&S acceptability is something relative to different V&V Users/Sponsors: what is acceptable to one V&V User/Sponsor may not be acceptable for another. The V&V User/Sponsor's decision-making process therefore requires appropriate evidence-based arguments to justify his or her acceptance decision.

The basic premise of GM-VV is that V&V are performed to collect, generate, maintain and reason with a body of evidence in support of the V&V Users/Sponsors acceptance decision-making process. Here, validation is referred to as the process that establishes the V&V User/Sponsor's confidence as to whether or not they have built or procured the right M&S system or result for the intended use (i.e., M&S validity). In other words "Did we build the right M&S system?". To ensure that the M&S system or results at delivery can be demonstrated to be valid, it is necessary to ensure that the M&S system is built and employed in the right manner. Here verification is referred to as the process of establishing V&V User/Sponsors confidence in whether the evolving M&S system or result is built right (i.e., M&S correctness). In other words "Did we build the M&S system right?". The GM-VV considers V&V as a specific problem domain of M&S with its own needs, objectives and issues. This domain is referred to as the V&V World (Fig. 6).

The V&V world groups the products, processes and organizational aspects that are needed to develop an acceptance recommendation that can be used by the V&V User/Sponsor in his or her acceptance decision procedure(s). This recommendation included in a V&V report is the key deliverable of a V&V effort and contains evidence-based arguments regarding the acceptability of an M&S system or results. Here the GM-VV premise is that the acceptance decision itself is always the responsibility of the V&V User/Sponsor and decision procedure(s) may involve trade-off aspects beyond the V&V effort scope.

The development of an acceptance recommendation in the V&V world is driven by the V&V needs that are traceable to the V&V User/Sponsor's acceptance decision or procedure(s) needs (e.g., budget, responsibilities, risks, liabilities). Therefore, the extent, rigor and timeframe of a V&V effort depend on these needs. Depending on these needs, the V&V effort could span the whole or specific M&S lifecycle phase of the four worlds; could focus on one specific or multiple (intermediate) M&S products; and should match the development paradigm that was used (e.g., waterfall, spiral). Each case may require a separate acceptance recommendation with its own scope and development timeline. Moreover, the way the V&V effort interacts with the four M&S-based problem worlds also varies from

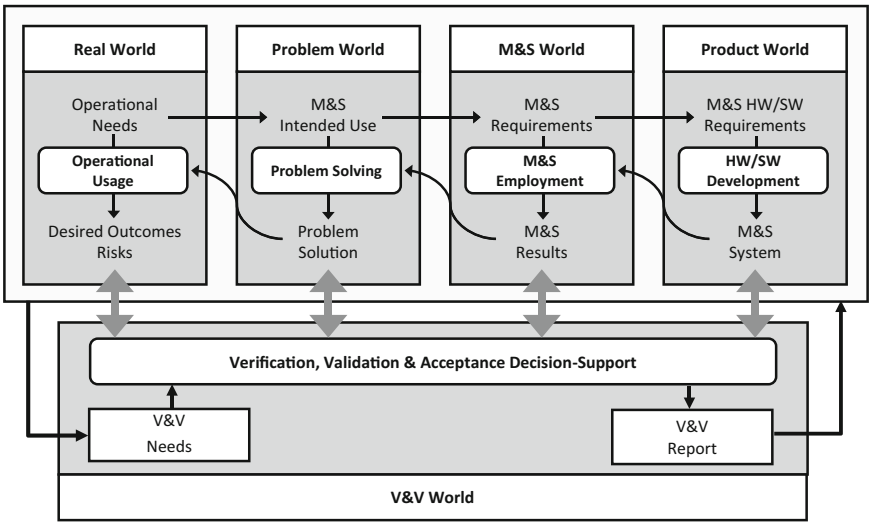


Fig. 6 V&V world and four-world interfacing

case to case. These mutual dependencies are depicted in Fig. 6 with bidirectional arrows that interface the V&V world with each of the four M&S-based problem solving worlds. Two classical types of V&V that can be identified based on the time frame of their execution are [6, 10–12]:

- **Post hoc V&V**: V&V conducted in retrospect on an M&S system after development or on M&S results after M&S system employment.
- **Concurrent V&V**: V&V conducted in prospective throughout the whole M&S life cycle to manage and improve the quality of newly developed M&S systems or results.

The GM-VV supports both V&V time frames but is not limited to these distinct types. A V&V effort can be post hoc, concurrent, iterative, recursive or even be a recurrent effort in the case where legacy M&S products are updated or reused for a different intended-use.

2.1.4 Acceptance Recommendation, Acceptability Criteria and Evidential Quality

The objective of a V&V effort is to develop evidence upon which an acceptance recommendation is based. This V&V objective is articulated as an acceptance goal. This high-level goal should be translated into a set of concrete and assessable acceptability criteria for the M&S system or result(s). Relevant and convincing

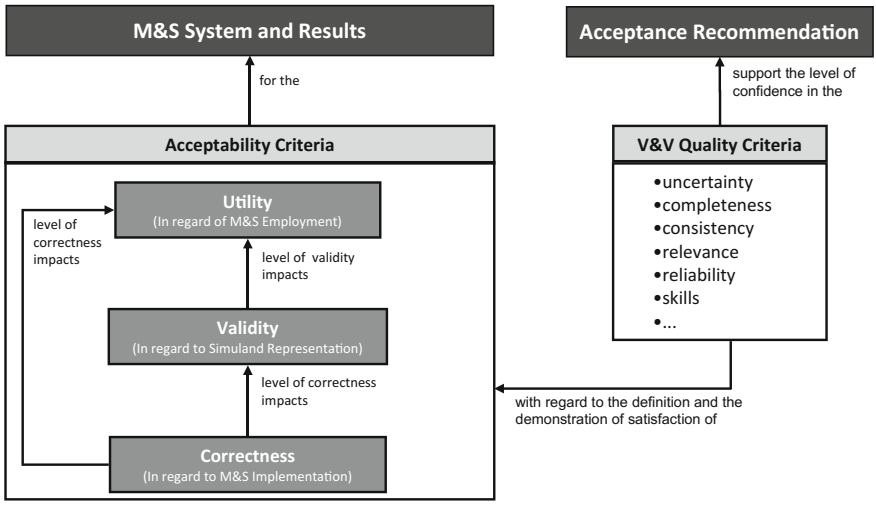


Fig. 7 Utility, validity, correctness and V&V quality criteria relationships

evidence should then be collected or generated to assess the satisfaction of these criteria. When it is convincingly demonstrated to what extent the M&S system or result(s) does or does not satisfy all these acceptability criteria, a claim can be made on whether or not the M&S system or result(s) is acceptable for its intended use (i.e., acceptance claim).

The GM-VV identifies three types of M&S properties for which acceptability criteria could be set (Fig. 7):

- **Utility**: this property refers to the extent to which the M&S system or result(s) is useful in solving the M&S user/sponsor's needs. Utility properties could comprise sub-types such as M&S value (e.g., measures of effectiveness, measures of performance), cost (e.g., money, time) and use risks (e.g., impact, ramifications).
- **Validity**: this property refers to the extent to which the M&S system's representation corresponds to the simulated simuland (i.e., system of interest) from the perspective of the intended use. The level of validity impacts the utility.
- **Correctness**: this property refers to the extent to which the M&S system implementation conforms to its specifications (e.g., conceptual model, design specification); and is free of design and development defects (e.g., semantic errors, syntactic errors, numerical errors, user errors). The level of correctness impacts both validity and utility.

These three types of M&S properties include but not limited to capability, accuracy, usability and fidelity [13, 14]. To make an acceptance decision, the V&V User/Sponsor needs to know whether the M&S system or results are (un)acceptable, as well as the evidential value of this acceptance claim (i.e., strength). The required evidential strength to establish sufficient trust in such a claim depends on the use

risks and the V&V User/Sponsor responsibilities (i.e., liability). The convincing force that can be placed on such a claim depends on the quality of the whole V&V effort. For this purpose, the GM-VV identifies quality properties that can be associated with identifying and defining the acceptability criteria; and developing convincing evidence for demonstrating their satisfaction (Fig. 7).

- **V&V Quality**: this property refers to how well the V&V effort is performed (e.g., rigor) with regard to developing the acceptability criteria, collecting evidence, and assessing to what extent the M&S satisfy the acceptability criteria (e.g., evidential value, strength).

Typical examples of V&V quality properties are the completeness, correctness, consistency, unambiguous and relevance of the acceptability criteria or their supporting items of evidence. In the process of collecting or generating evidence, quality properties could comprise independence of applied V&V techniques or persons, knowledge gaps and uncertainties of referent data for the simuland [15], skill level of V&V personnel, and reliability and repeatability of V&V techniques. Relevance and warrants for any assumption made in a V&V effort could also be addressed in the form of quality properties.

The defined acceptability criteria, the collected evidence and assessment of the satisfaction of these criteria are the basis for developing the arguments underlying the acceptance claim. This acceptance claim provides the V&V User/Sponsor with a recommendation regarding the acceptability of the M&S system or result for the intended use. In practice, an acceptance recommendation is not necessarily just a yes or no claim, in the sense that an M&S system or results can be accepted only if it meets all of the acceptability criteria and cannot be accepted if it does not. Meeting all the acceptability criteria means the claim can be made that the M&S system or result should be accepted to support the intended use without limitations. In case not all acceptability criteria are met, alternative weaker acceptance claims with underlying arguments can be constructed. Such alternative acceptance claims could, for example, provide recommendations regarding conditions or restrictions under which the M&S system or result can still be used (i.e., limit the domain of use); or on modifications that, when implemented, will lead to an unconditionally acceptable M&S system or results for the intended use. Another rationale for alternative acceptance claims is when convincing or sufficient evidence is lacking (e.g., access to data prohibited, or referent system unavailable for testing). In any case, an acceptance recommendation always requires well-structured supporting arguments and evidence for the V&V User/Sponsor to make the right acceptance decision. Depending on the identified M&S use risk, the V&V User/Sponsor can also decide not to take any actions when not all acceptability criteria are met by the M&S system. In that case, the V&V User/Sponsor simply accepts the risks associated with the M&S system use.

2.1.5 V&V Argumentation Approach: Structured Reasoning with Arguments

Developing an acceptance recommendation that meets the V&V User/Sponsor needs usually involves the identification and definition of many interdependent acceptability criteria, particularly for large-scale and complex M&S systems or for M&S-based solutions used in safety–critical, real-world environments. Demonstrating the satisfaction of acceptability criteria requires evidence. Collecting the appropriate evidence is not always simple and straightforward, or even not always possible due to various practical constraints (e.g., safety, security, costs, schedule). In many cases, the collected evidence comprises a large set of individual items or pieces of evidence that may be provided in different forms or formats, and may originate from various sources (e.g., historical, experimental data, SME opinion). Moreover, the strength of each item of evidence may vary and the total set of collected evidence may even contain contradicting items of evidence (i.e., counter evidence). The quality of this effort determines the value of an acceptance recommendation for the V&V User/Sponsor. Therefore, the arguments underlying an acceptance recommendation should be developed in a structured manner using a format where the reasoning is traceable, reproducible and explicit. Alternative approaches to implement such reasoning exist and may be incorporated within the GM-VV technical framework to tailor it the specific needs of an M&S organization or domain. An example of such an approach is the V&V goal-claim network approach (Fig. 8). A V&V goal-claim network is an information and argumentation structure rooted in both goal-oriented requirements engineering and claim-argument-evidence safety engineering principles [16–19].

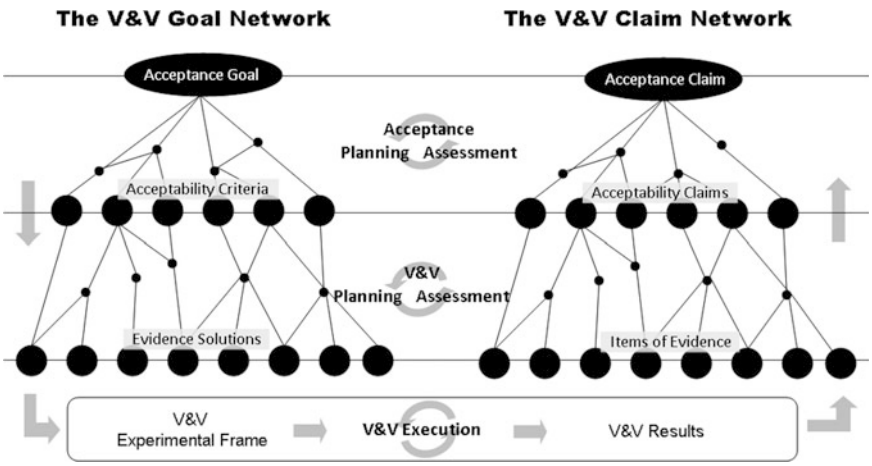


Fig. 8 V&V goal—claim network

Figure 8 provides an abstract illustration of a V&V goal-claim network. The left part of the goal-claim network is used to derive the acceptability criteria from the acceptance goal; and deriving solutions for collecting evidence to demonstrate that the M&S asset satisfies these criteria as indicated by the top-down arrows. The acceptance goal reflects the V&V needs and scope (e.g., simuland, intended use). Evidence solutions include the specification of tests/experiments, referent for the simuland (e.g., expected results, observed real data), methods for comparing and evaluating the test/experimental results against the referent. Collectively, they specify the design of the V&V experimental frame used to assess the M&S system and its results. When implemented, the experimental frame produces the actual V&V results. After a quality assessment (e.g., for errors, reliability, strength), these results can be used as the items of evidence in the right part of the goal-claim network. These items of evidence support the arguments that underpin the acceptability claims. An acceptability claim states whether a related acceptability criterion has been met or not. Acceptability claims provide the arguments for assessing whether or to what extent the M&S system and its results are acceptable for the intended use. This assessment, as indicated by the bottom-up arrows in Fig. 8, results in an acceptance claim inside the V&V goal-claim network. As such a V&V goal-claim network encapsulates, structures and consolidates all underlying evidence and argumentation necessary for developing an appropriate and defensible acceptance recommendation. The circular arrows in Fig. 8 represent the iterative nature of developing a V&V goal-claim network during planning, execution and assessment phases of a V&V effort.

2.1.6 V&V Organizational and Management Approach

In order to facilitate efficient and high quality V&V, the V&V effort inside the V&V world should be executed in a controlled and organized way. The basic premise of the GM-VV is that the acceptance recommendation for an M&S asset is developed and delivered by means of a managed project. Moreover, GM-VV assumes that V&V is conducted by a person, a team of people or a dedicated organization with assigned responsibilities, obligations and functions. Therefore, GM-VV identifies three organizational levels at which V&V efforts can be considered. In order of the lowest to the highest organizational level these levels are:

- Technical Level: concerns the engineering aspects of a V&V effort that are necessary to develop and deliver an acceptance recommendation,
- Project Level: concerns the managerial aspects related to the proper execution of the technical actions of a V&V effort,
- Enterprise Level: concerns the strategic and enabling aspects to establish, direct and support the execution or business environment for V&V efforts.

The core GM-VV concept on the V&V project level is the concept of a managed project. A V&V project can be viewed as a unique process comprised of coordinated and controlled activities that address: V&V effort planning in terms like cost, timescales and milestones; measuring and checking progress against this planning; and selecting and taking corrective actions when needed. A V&V project could be a separate project alongside the M&S project of which the M&S asset is part, or be an integral part of this M&S project itself (e.g., subproject, work package). A separate V&V project is particularly relevant in the case when a level of independence must be established between the M&S development and V&V team/organization. On the V&V project level, GM-VV also provides derived concepts such as a V&V plan and report to manage the technical V&V work.

For CIPRNet all three levels are important. For CI it is important to have a good set of tools and techniques to do the technical V&V activities. Since with the application of M&S systems for serious CI application there is always M&S Use Risk involved, for each project run by the to be established EISAC (European Infrastructures Simulation and Analysis Centre), V&V activities should be executed. A project approach is suited for that. Doing V&V from within EISAC means that EISAC should have support for the V&V activities at the highest level: the enterprise level.

The core GM-VV concept on the V&V enterprise level is the concept of an enterprise entity. A V&V enterprise entity can be viewed as an organization that: establishes the processes and lifecycle models to be used by V&V projects; initiates or defers V&V projects; provides resources required (e.g., financial, human, equipment); retains reusable knowledge and information from current V&V projects; and leverages such knowledge and information from previous V&V projects. The V&V enterprise provides the environment in which V&V projects are conducted. GM-VV defines two types of enterprise entities:

- **V&V Client**: the person or organization that acquires V&V products or services,
- **V&V Supplier**: the person or organization that develops and delivers V&V products or services.

A V&V agreement is arranged between a V&V client and V&V supplier to provide products and/or services that meet the V&V client's needs. Both these V&V entities could be organizations (e.g., companies) separate from the organization that develops or acquires M&S or it could be different units (e.g., department, division, group) within a single M&S supplier or client organization. Typically, a separate V&V supplier is an organization that has the provision of independent V&V products and services to external V&V clients as its core business. Though depending on their business model, an M&S supplier or client organization could have their own V&V supplier entity that may provide V&V services and products to internal and external V&V clients alike.

2.1.7 V&V Levels of Independence: Acceptance, Certification and Accreditation

An independent V&V (IV&V) authority is often described as an organization or a person that is employed to conduct V&V, independent of the developer's team or organization [6, 10, 12]. The need for IV&V is mostly driven by:

- risks and liabilities taken by the V&V User/Sponsor's acceptance decision,
- level of trust the V&V User/Sponsor has in the M&S developer,
- authoritative policies and regulations that may demand independent V&V for the M&S intended use,
- lack of specialist skills, tools and techniques by user, sponsor or developer to perform V&V.

In practice however, it is highly incumbent upon the V&V User/Sponsor acceptance decision needs and complexity of the M&S system as to which parts and to what extent V&V should be conducted in an independent manner. Therefore, the GM-VV adopts a sliding scale of independence for V&V [15], which can be selected accordingly to match the V&V needs. The justification and selection of a proper level of independence is supported within GM-VV through the use of the V&V argumentation network. Within this sliding scale for independent V&V, certification and accreditation can be located in the right part of the scale (Fig. 9).

2.1.8 V&V Information and Knowledge Management

V&V of M&S is an information and knowledge intensive effort. In particular, during the V&V of large scale, distributed or complex M&S applications, care must be taken to preserve or reuse information and knowledge. Therefore, GM-VV

Fig. 9 Levels of independent V&V

applies the memory concept on both the V&V project and enterprise levels. A memory is viewed as a combination of an information and knowledge repository and a community of practice [20]. The repository is a physical place where information, knowledge objects, and artefacts are stored. The community of practice is composed of the people who interact with those objects to learn, understand context and make decisions.

The V&V project memory provides the means to manage information and knowledge produced and used during the lifetime of an individual V&V project. V&V is often an iterative and recurrent process linked to an M&S system's life-cycle, hence V&V products for an M&S system may have different configurations. Therefore, a V&V project memory may also retain records on possible different V&V product configurations. The V&V enterprise memory retains the total body of information and knowledge from past and current V&V projects to sustain and support the cost-effective execution of future V&V projects. Such reusable information could be, for example, M&S technology or domain specific recommended practices, acceptability criteria, V&V goal-claim network design patterns, V&V tools and techniques, or policies and standards. On a more strategic level, a V&V enterprise memory could retain information and knowledge on V&V project costs and maturity as well.

2.2 *Implementation Framework*

The GM-VV implementation framework translates the GM-VV basic concepts into a set of generic V&V building blocks (i.e., components). These may be used to develop a tailored V&V solution that fits the V&V needs of any particular M&S organization, project, application, and technology or problem domain. The implementation framework has three interrelated dimensions: product, process and organization (Fig. 10). The underlying principle of this framework is that the V&V needs of the V&V User/Sponsor in the M&S four-world view are addressed by one or more V&V products, those being the V&V report and possibly other custom V&V products the V&V User/Sponsor may need. These V&V products in general require intermediate products (i.e., information artefacts) and associated processes to produce them. The V&V processes are executed by a corresponding V&V organization that is responsible for the development and delivery of the V&V products. In general the V&V effort should result in a V&V report to be delivered to the customer containing one or more of the information artefacts. Individual needs will drive which V&V products are required.

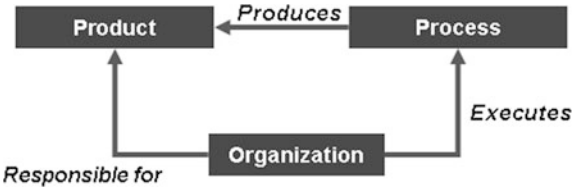


Fig. 10 GM-VV implementation framework dimensions

As indicated in Fig. 10, the GM-VV implementation framework consists of three key dimensions:

- **Products**: the information artefacts that may be delivered, developed or used throughout a V&V effort. These artefacts can have multiple instances, representational and documentation formats.
- **Processes**: the set of activities and tasks that comprise V&V execution as well as those management tasks that increase the efficiency and effectiveness of the V&V effort. These activities and tasks are inspired by the IEEE standard system life-cycle processes model [2] and can be carried out recursively, concurrently, and iteratively.
- **Organization**: the roles played either by people or by organizations in the V&V effort. The roles are defined in terms of responsibilities and obligations. Depending on the M&S organization, project and application domain needs; several roles could be played by separate organizations, separate people in one organization or by a single person.

The V&V effort culminates in a V&V report that is comprised of the information generated throughout the execution of the V&V and acceptance decision-support process (Fig. 6). The following sub-sections provide an overview of the information artefacts, activities and roles that are implemented or produced during this execution. They are ordered according to the GM-VV technical, project and enterprise levels.

It is important to re-emphasize the tailorable nature of the methodology. GM-VV provides all the elementary information artefacts, activities, tasks and roles to address the most common technical, project and enterprise level aspects of a V&V effort. Depending on the M&S project and organizational needs one could choose not to implement all GM-VV components or one could choose to adjust them accordingly. This is particularly relevant for M&S organizations that already have some project and enterprise level components in place, and only require technical level V&V (intermediate) products, processes and roles to conduct their V&V effort. The overall tailoring and application concepts of the GM-VV implementation framework are provided in the next section.

2.3 Tailoring Framework

GM-VV recognizes that a particular M&S organization, project, application, technology or problem domain may not need all these components or use them directly as-is. Therefore, the GM-VV components are intended to be selected, combined and modified accordingly, to obtain an effective and efficient V&V effort of sufficient rigor. This is particularly relevant for M&S projects and organizations that already have some project and enterprise level components in place, and only require technical level V&V (intermediate) products, processes and roles to conduct their V&V effort.

The basic premise of the GM-VV tailoring concept is that the GM-VV should first be cast into a concrete V&V method fit for an organization or application domain, and secondly this instance should be optimized for a V&V project. This tailoring concept is implemented by means of a framework that refers to all three levels of the GM-VV implementation framework. The objective of this GM-VV tailoring framework is to adapt each GM-VV (intermediate) product, process and role to satisfy the specific requirements and constraints of:

- An organization that is employing the GM-VV (e.g., company policies, standards)
- A domain in which the GM-VV is employed (e.g., standards, regulations, technologies)
- A V&V supplier entity delivering V&V products or services (e.g., standards, processes)
- A V&V project (e.g., time, budget, scale, complexity, risk, resources).

As described above tailoring is accomplished in two phases. In the first phase of the GM-VV tailoring framework, the implementation framework components are utilized to establish concrete V&V solution instances on one or more of the three organizational levels (i.e. a permanent V&V organization, V&V project or technical V&V approach). In here, the GM-VV recognizes that a particular M&S organization, project, technology or problem domain may not need all three organizational levels or all components on a single organizational level nor even use them directly as-is. Therefore, the GM-VV implementation framework organizational levels and components are selected, combined and modified accordingly, to obtain a concrete tailored V&V solution. For instance an M&S organization may already have an M&S project and enterprise level in place, and only require technical level V&V (intermediate) products, processes and roles to conduct their technical V&V work. Successful application of the first phase of the tailoring framework results in a modified or new V&V solution instance conforming to the GM-VV architectural templates (i.e. in a structure and organizational manner). Four tailoring approaches can be used for this: extension, omission, specialization and balancing, which are discussed below.

In the second phase these same tailoring approaches are applied throughout the operational lifetime (i.e. permanent organization or project) or execution (i.e. technical approach) of each V&V solution instance. This type of tailoring comprises run-time optimization of the instantiated V&V processes at all three organizational levels. At a technical level this could imply the application of a risk-based V&V approach, such as the MURM [21], to prioritize the acceptability criteria, allocate and specific V&V techniques and tools based on V&V User/Sponsor risk tolerance levels. On the project level this could be the alignment of technical V&V activities with the progress of the M&S system's life-cycle phases, balance and allocate the available V&V resources to each phase M&S life-cycle or (work) products. On the enterprise level this could mean balancing the

cost-risk of new investments in training of personnel or V&V tool infrastructure development against a future V&V project order intake volume.

The GM-VV tailoring framework applies four basic tailoring approaches:

- **Tailoring by Extension**: adaptation of the implementation framework by adding custom V&V products, processes, activities, tasks and roles. For example, a V&V Client organization or application domain may require additional custom artefacts not foreseen by the GM-VV.
- **Tailoring by Reduction**: adaptation of the implementation framework by deleting products, processes, activities, tasks and roles due to constraints such as inaccessibility of data and information protected by intellectual property rights, security or technical restrictions.
- **Tailoring by Specialization**: adaptation of the implementation framework by adding or using domain specific V&V methods, techniques and data that are unique for a V&V project, organization or application.
- **Tailoring by balancing**: adaptation of the implementation framework by fitting a suitable cost-benefit-ratio towards an acceptance recommendation. The level of acceptable M&S use risk should drive the rigor and resources employed for V&V. Therefore, in this approach one tries to balance aspects such as:

  – M&S use-risk tolerances and thresholds
  – criticality and scope of the acceptance decision
  – scale and complexity of the M&S system
  – information security, with

  V&V project resource variables such as

  – time schedule
  – budget
  – V&V personnel skills
  – infrastructure.
  – Hence, balancing establishes the suitable and feasible level of rigor for the V&V effort.

Tailoring by these four approaches should be performed in accordance with the three dimension design principle of the GM-VV implementation framework (Fig. 10), to obtain a consistent and coherent V&V method and project. For example, each new or specialized product needs a corresponding process (activities, tasks) and role (responsibilities, obligations).

Successful application of the tailoring framework results in a modified or new V&V method instance conforming to the GM-VV. This consists of concrete V&V organization, products and processes, which should achieve the V&V objectives of an M&S organization, project, technology, or application domain.

The first three types of tailoring are mainly of importance at the start of a V&V effort. The tailoring by balancing is important during the V&V effort.

2.3.1 Risk Decomposition and Tailoring by Balancing

As described above it is advised to use a decomposition of the top goal into smaller and smaller goals up to the point that a test can be devised that is within resources and is likely to deliver suitable evidence. During the balancing tailoring during the execution of the V&V work priorities need to be determined. These priorities together with the resources available are used to decide which goals will be further expanded and which will be left undeveloped. The basis for that decision and thus for the prioritization is risk. What is needed is to determine the contribution of a goal to the overall M&S use-risk. If a goal has a high contribution of risk it must be taken into consideration in the V&V work. If it has a very low contribution it can. In that case it should be explicitly be recorded that that goal is not used in the rest of the V&V work such that at the end a feeling for how complete the V&V work is can be obtained.

An evidence solution for a goal with a (relatively) high contribution to the overall risk should likely result in a high confidence in the evidence. For a goal with a low contribution to the M&S use-risk risk it may be sufficient to have evidence that contains some uncertainty, i.e. if the evidence is just an indication that the goal is met it may already suffice.

To find the contribution to the overall M&S use risk for a node it is necessary to make a risk decomposition in the same way as the decomposition of the Acceptance Goal, see Fig. 8. In practice it is difficult to make an exact risk decomposition, therefore it is advised to use a somewhat simpler approach as indicated in Fig. 11. The red stands for high contribution to the overall M&S use risk, orange for medium contribution and green for low contribution. During the decomposition nodes with a low contribution to the overall use risk may be left undeveloped. At the bottom of Fig. 11 the contribution to the risk is an indication of how convincing the evidence should be which is important for specifying which type of tests are required.

If after evidence collection it turns out not all goals are met, the contribution to the overall risk may be used during the acceptance decision to decide what to do. If it concerns a node with low contribution to the overall M&S use risk, it may be decided to leave things as is and accept the small risk. If it is goal with a medium or

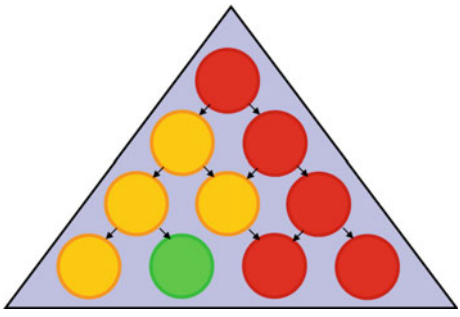


Fig. 11 Risk decomposition

high contribution to risk it can be decided to either change the M&S system such that the identified problems are corrected, or the purpose for which the user intends to use the M&S System should be made smaller such that the current state of the M&S System will be fit for purpose.

2.4 Why Is This Structured Approach so Much More Effective and Efficient

The above-described structured approach to doing V&V has a number of advantages that make it more effective and more efficient than doing V&V in a less structured way. Below some of the key advantages are discussed.

The right starting point for the V&V effort leads to more effective results
The V&V effort should start from the perspective of risk. Who runs the real risk in an M&S endeavour? It is not the modeller, not the implementer (maybe there is a risk of repetitive strain injury) and not the person who executes the simulation (maybe if there is a moving base simulator). In general the real M&S use risk is found when the M&S based results are applied in the real word. Therefore V&V processes that are developer oriented might miss the real risk. Also, when studying the 4-world view in Fig. 5 it may become clear that possibly many more aspects may need to be considered than just the domain knowledge as coded in a simulation. Thus organizational aspects that may make or break the use of simulation, the level of proficiency of all people involved, the processes used to derive the products such as the Operational Needs, etc. may all play a significant role and may need to be included in determining the overall utility and thus in the V&V approach. If such a very broad scope is used it becomes clear that a domain oriented V&V process may also miss some aspects. Therefore a general methodology that starts at the true M&S use risk and that can incorporate domain specific elements as well as other aspects will result in a more effective V&V result because the right starting point can be chosen and all relevant aspects included.

Balancing resources with needs leads to efficiency and effectiveness
A structured decomposition of the Acceptance Goal into all aspects that are relevant and on top of that a decomposition of the contribution of the M&S use risk attached to the Acceptance Goal leads to the possibility to spend the available resources for the V&V effort wisely. Based on priorities related to the contribution to the overall M&S use risk it can be decided which parts of the decomposition requires more or less effort. When available resources do not allow testing all aspects to their maximum, i.e. in all practical situations, it can be decided to let the goals with low contribution to risk remain undeveloped. In that case it should be explicitly recorded that that goal is not used in the rest of the V&V work, see "Knowledge of the completeness of the V&V effort leads to effectiveness" below. If nodes are developed to the point where tests can be defined, the contribution to the M&S use risk can be used to make choices for tests. Low contribution to the risk allow for cheaper tests

that may not give a high convincing force. A high contribution to the risk means that sufficient convincing force must be required of the evidence, possibly meaning more expensive tests need to be performed.

The structured approach to V&V makes it possible to balance the resources during the construction of the goal network and the evidence solutions. This means that the V&V effort uses the available resources in an efficient way, allowing for the best possible answer for the given resources, which means the highest possible effectiveness.

Re-usable domain knowledge leads to more efficient and effective results
The top part of the decomposition of the Acceptance Goal, see Fig. 8, contains domain knowledge because it is the user's perspective that is encoded and the role of the M&S system in that domain. From an V&V enterprise point of view, see Sect. 2.1.6, this domain knowledge can be re-used if other V&V projects are executed on (almost) the same domain or for (almost) the same purpose. In that case the domain knowledge can be re-used and even extended to be more complete. Of course, for each new project in which existing domain knowledge is re-used it must be made sure that no irrelevant aspects are taken into account. Over the course of several projects the domain knowledge becomes more and more complete, which helps in not forgetting possibly important aspects. The re-use of domain knowledge thus leads to more to a more effective and more efficient V&V effort. It is, however, needed that a good discipline in documenting the V&V effort is used.

Distribute the V&V work among experts leads to efficiency
In the lower part of the goal-network many different aspects covering many different disciplines can be found. The expansion—if needed—of these goals and the execution of associated tests likely requires different experts and facilities. Using the natural break up of a structured approach to V&V, e.g. the tree structure in Fig. 8, it becomes easier to assign experts to different groups of goals and tests. For CI simulation it may be that organizations do not wish to have other experts test their simulation assets, in that case each partner can be assigned a set of goals for which they need to provide evidence. It would be better, however, to have a certain level of independence (see Sect. 2.1.7). The structured approach leads to more efficient execution of the V&V effort by clearly indicating which expertise should be handled by which expertise.

Complete one branch while waiting for others to complete leads to efficiency
In the structured approach as presented above, it becomes clear that if one branch of the tree structure is fully developed and ready for execution of the tests, there may be no need to wait for other parts to also become fully developed. The parts that are ready to go to the test phase can start independently of the rest. This may even lead to the discovery of problems with the M&S System that can already be corrected before tests of other branches are executed. This leads to a more overall efficient V&V effort.

Knowledge of the completeness of the V&V effort leads to effectiveness
During the balancing of the resources in building the goal network and the specification of the evidence solutions the important decisions on when goals with a low

contribution to the M&S use risk are left undeveloped and which tests are chosen in the specification of the evidence solutions should be unambiguously be recorded. That makes it possible to get a feeling for how complete the V&V effort as a whole is. This completeness should be translated into an uncertainty in the Acceptance Recommendation to the customer. Thus if insufficient resources were allocated to the V&V work, the conclusion might state that the available evidence indicates that the M&S system is fit for purpose, but that the V&V effort as a whole has left too many aspects out of consideration and that thus a high level of uncertainty is present in that statement.

The statement on completeness of the V&V effort will allow the decision maker to make a much better decision, which leads to better effectiveness of the use of the V&V results.

Standardized documentation leads to efficiency
An often observed problem with unstructured V&V efforts is that it results in either very little documentation or it results in a lot of documents that are unorganized and scattered over different places, usually in the form of computer files that are difficult to find and for which it is hard to recall what its content means and in what piece of evidence it was used.

A structured approach should adopt some standard approach to documentation. This documentation should be such that the Acceptance Recommendation should be completely traceable through the claim network, via the evidence collection, through the goal network back to the Acceptance Goal. Also all decisions due to tailoring should be well documented and immediately clear where they influence the Acceptance Recommendation.

A standardized approach to documentation is also important on the V&V enterprise level where it can be expected that re use of previous V&V projects will lead to efficiency.

Efficiency for recurrent testing
In practice it may occur that a M&S system had been used for some time and that subsystems are being replaced or upgraded. In that case the structured approach described above makes it immediately clear which parts of the goal network are affected by the change and which tests should be re-done for the new M&S system. This leads to a very efficient way of doing recurrent testing.

3 Choose the Appropriate Verification and Validation Technique

There are many different V&V techniques, see e.g. [22–25]. The V&V techniques in those references are categorized in Table 1.

Table 1 Examples of V&V techniques

Informal	Formal	Static	Dynamic
• Audit • Desk checking • Documentation checking • Face validation • Inspections • Reviews • Turing test • Walkthroughs	• Induction • Inductive assertions • Inference • Logical deduction • Lambda calculus • Predicate calculus • Predicate transformation • Proof of correctness	• Cause-effect graphing • Control analysis • Calling structure analysis • Concurrent process analysis • Control flow analysis • State transition analysis • Data analysis • Data dependency analysis • Data flow analysis • Fault/failure analysis • Interface analysis • Model interface analysis • User interface analysis • Semantic analysis • Structural analysis • Symbolic evaluation • Syntax analysis • Traceability assessment	• Acceptance testing • Alpha testing • Assertion checking • Beta testing • Bottom-Up testing • Comparison testing • Compliance testing • Authorization testing • Performance testing • Securitytesting • Standards testing • Debugging • Execution testing • Execution monitoring • Execution profiling • Execution tracing • Fault/failure insertion testing • Field testing • Functional (Black-Box) testing • Graphical comparisons • Interface testing • Data interface testing • Model interface testing • User interface testing • Object-flow testing • Partition testing • Predictive validation • Product testing • Regression testing • Sensitivity analysis • Special input testing • Boundary value testing • Equivalence partitioning testing • Extreme input testing • Invalid input testing • Real-time input testing • Self-driven input testing • Stress testing • Trace-driven input testing • Statistical techniques • Structural (White-Box) testing

(continued)

Table 1 (continued)

Informal	Formal	Static	Dynamic
			• Branch testing • Condition testing • Data flow testing • Loop testing • Path testing • Statement testing • Submodel/module testing • Symbolic debugging

The four broad categories of V&V techniques can be described as:

- **Informal V&V techniques** are usually executed and interpreted by humans. Typically these require few resources and can be executed in a short time. The convincing force, however, depends on the trust in the humans doing the work and the process they use.
- **Formal V&V techniques** are based on mathematical proofs of correctness. The application of formal methods, however, is often limited due to large resource costs even for relatively small M&S systems and their use. If applicable, the convincing forces of the V&V results are very strong.
- **Static V&V techniques** can be applied early in the development process because no execution is required. It is typically applied in the concept phase and parts of the development phase. Typically specialized tools are used to do automated checks. The required resources are normally limited. It is required to have access to documentation and half-products. The strength of the convincing force is dependent on the rigor of the tests.
- **Dynamic V&V techniques** require execution of the M&S System in part or as a whole. The dynamic properties of the M&S System are studied and checked. Typically specialized tools are used to do automated measurements and checks. The required resources are normally limited. Dynamic V&V techniques may require access to parts of the M&S System that are usually not available. The strength of the convincing force is dependent on the rigor of the M&S System check.

It is difficult to state in general which V&V techniques (i.e. what type of tests) should be used. So in this text we provide a basis to choose the right V&V technique. There are a number of important aspects that determine which V&V techniques are appropriate for a given situation:

- Contribution to the M&S Use Risk
  - It is clear that a relatively high contribution to the M&S Use Risk requires evidence that can be trusted. This requires a rigorous V&V technique, i.e. one for which the expected residual uncertainty is low. When possible formal techniques should be used. In practice however, this is often prohibitively

expensive and (combinations of) techniques have to be used that are with the available means but still deliver sufficiently trustworthy evidence.

- Available means
  - The available means are a set of limiting factors such as budget, time, expert knowledge, access to testing facilities, etc. The whole V&V effort has to be run within these limits. That means that during the construction of the goal network only those criteria can be considered that contribute highly to the over M&S Use Risk and collectively are likely to remain within the available means. The collection of evidence solutions has to be chosen such that the expected results of executing the tests delivers the lowest overall residual uncertainty.
- Referent data
  - The Referent data is the knowledge of the real world. It is needed during the tests to compare the simulation results with. If no or little referent data is available only tests that do not (heavily) depend on referent data can be chosen, e.g. expert opinion or examination of the conceptual model.
- M&S system availability
  - For dynamic testing it is evident that (parts of) the M&S system itself has to be available. Some types of tests require access to M&S system internals in order to make "measurements" that are not visible to the end user. For other tests it is necessary to have access to development documents such as the conceptual model.

Summarizing: the tests all have different costs and different expected residual uncertainty. The contribution to the M&S User Risk should be the basis for choosing the best V&V techniques. A set of evidence solutions need to be chosen such that collectively the best possible result for the given available resources is obtained.

Take away message: You have to choose the appropriate Verification and Validation techniques to balance risk, effectiveness and efficiency.

4 Conclusion

As a very brief summary of the text above it can be stated that:

- You have to do Verification and Validation because there is risk involved,
- You have to do it in a structured way if you want to do it more effective and more efficient,
- You have to choose the appropriate Verification and Validation technique to balance risk, effectiveness and efficiency.

Acknowledgement and Disclaimer This chapter was derived from the FP7 project CIPRNet, which has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no. 312450.

The contents of this chapter do not necessarily reflect the official opinion of the European Union. Responsibility for the information and views expressed herein lies entirely with the author(s).

References

1. SISO (2012) GM-VV Vol. 1: introduction & overview, SISO-GUIDE-001.1-2012
2. IEEE, Systems and software engineering—system life-cycle processes, IEEE Std 15288-2008, Jan 2008
3. DoDI 5000.61, DoD modeling and simulation (M&S) verification, validation, and accreditation (VV&A), 9 Dec 2009
4. Roza M, Jacquart J, Giannoulis C (2009) Common validation, verification and accreditation framework for simulation, REVVA-2 Reference Manual. Report: Europa 111–104. Mar 2009
5. IEEE, IEEE recommended practices for verification, validation and accreditation of a federation—an overlay to the high level architecture (HLA) FEDEP, IEEE Std 1516.4-2007, Dec 2007
6. US DoD, Safety Management College, Systems engineering fundamentals, SEF-Guide 01-01
7. Wasson CS (2006) System analysis, design and development: concepts, principles and practices. Wiley, Hoboken
8. INCOSE (2002) Systems engineering handbook, a "How To" guide for all engineers. Version 2.0. INCOSE
9. Grady JO (1998) System verification and validation. CRC Press LLC, Boca Raton
10. US Department of Defense Verification, Validation, and Accreditation Recommended Practices Guide, RPG Build 4.0, Nov 2011. http://vva.msco.mil/
11. UK MoD, A generic process for the verification & validation of modeling and simulation & synthetic environments systems, DEF STAN 03-44 Issue 2, 31 Mar 2008
12. Australian DoD (2005) DSO, Simulation verification, validation and accreditation guide
13. Gross DC et al (1999) Report from the fidelity implementation study group. 1999 Spring SIW Proceeding, 99S-SIW-167
14. Roza ZC (2004) Simulation fidelity theory and practice: a unified approach to defining, specifying and measuring realism of simulations. Delft University Press Science, Delft
15. Oberkampf WL, Roy CJ (2010) Verification and validation in scientific computing. Cambridge University Press, Cambridge
16. Lamsweerde van A (2001) Goal oriented requirements engineering: a guided tour. In: Fifth IEEE international symposium on requirements engineering
17. Anwer S, Ikram N (2006) Goal oriented requirement engineering: a critical study of techniques. In: XIII Asia Pacific software engineering conference
18. Kelly TP (1998) Arguing safety—a systematic approach to managing safety case. Master's thesis, University of York, Sept 1998
19. Mayo P (2002) Structured safety case evaluation: a systematic approach to safety case review. Master's Thesis, University of York
20. Wikipedia, Information management, information lifecycle management and knowledge management
21. Risk-based methodology for verification, validation and accreditation (VV&A): the M&S use risk methodology (MURM). Johns Hopkins University Applied Physics Laboratory Report, NSAD-R-2011-011, Apr 2011

22. Balci O (1997) Verification, validation, and accreditation of simulation models. In: Andradhttir S, Healy KJ, Withers DH, Nelson BL (eds) Proceedings of the 1997 winter simulation conference, pp 135–141
23. Sargent (2010) Verification and validation of simulation models. In: Johansson B, Jain S, Montoya-Torres J, Hugan J, Yücesan E (eds) Proceedings of the 2010 winter simulation conference, pp 166–183
24. DoD (2001) V&V techniques, RPG Reference Document, vva.msco.mil
25. Petty D (2011) Model verification and validation methods, I/ITSEC tutorial 1101

Chapter 9
Design of DSS for Supporting Preparedness to and Management of Anomalous Situations in Complex Scenarios

Antonio Di Pietro, Luisa Lavalle, Luigi La Porta, Maurizio Pollino, Alberto Tofani and Vittorio Rosato

Abstract Decision Support Systems (DSS) are complex technological tools, which enable an accurate and complete scenario awareness, by integrating data from both "external" (physical) situation and current behaviour and state of functioning of the technological systems. The aim is to produce a scenario analysis and to guess identify educated the most efficient strategies to cope with possible crises. In the domain of Critical Infrastructures (CI) Protection, DSS can be used to support strategy elaboration from CI operators, to improve emergency managers capabilities, to improve quality and efficiency of preparedness actions. For these reasons, the EU project CIPRNet, among others, has realised a new DSS designed to help operators to deal with the complex task of managing multi-sectorial CI crises, due to natural events, where many different CI might be involved, either directly or via cascading effects produced by (inter-)dependency mechanisms. This DSS, called CIPCast, is able to produce a real-time operational risk forecast of CI in a given area; other than usable in a real-time mode, CIPCast could also be used as scenario builder, by using event simulators enabling the simulation of synthetic events whose impacts on CI could be emulated. A major improvement of CIPCast is its capability of measuring societal consequences related to the unavailability of primary services such as those delivered by CI.

1 Introduction

The set of Critical Infrastructures (CI) constitutes nowadays an enabling pillar of societal life. They guarantee the supply of vital services (transport of energy products, telecommunication, drinkable water delivery, provide mobility functions)

A. Di Pietro (✉) · L. Lavalle · L. La Porta · M. Pollino · A. Tofani · V. Rosato
Laboratory for the Analysis and Protection of Critical Infrastructures,
ENEA Casaccia Research Centre, Rome, Italy
e-mail: antonio.dipietro@enea.it

R. Setola et al. (eds.), *Managing the Complexity of Critical Infrastructures*,
Studies in Systems, Decision and Control 90,
DOI 10.1007/978-3-319-51043-9_9

thus concurring to the achievement of citizens' (and societal as a whole) well-being. CI are complex technological or engineering systems: they are thus vulnerable as exposed to natural and anthropic-related events. Physical damages inflicted to CI elements might produce severe repercussions on their functioning which can reduce (or even reset) their functionality. Other than being individually wounded and functionally reset, they can propagate perturbations to other CI to whom they are functionally (inter-)connected. Connection and inter-connection are two relevant properties of systems of CI: connection indicates a one-direction supply mechanism, when one CI supplies a service to another. When such a service is no longer provided, the supplied CI may undergo a more or less severe perturbation. Inter-dependency indicates the presence of feedback loops: a CI might perturb other CI which, directly or through a further perturbation to other CI, could back-propagate the perturbation to the CI which initiates the perturbation cascade. This might produce a further functionality degradation which is amplify the negative feedback loop, by producing more and more serious effects. Cascading effects may spread perturbations on large geographical scales, on time scales ranging from a few second to days, producing reversible and, in some cases, irreversible societal effects.

Other than having repercussion on citizen activities, CI damages and the consequent services perturbation could affect the environment and produce large economic losses. Industrial activities are directly related to the supply of these services; their loss directly implies a lack of production and revenues contraction. In some cases, moreover, CI outages might produce environmental damages (gas release, spill of oil or other products, fires releasing toxic products, nanoparticles, ashes) that further increase the societal consequences.

As CI deliver relevant (in some cases, "vital") services to the citizens, their societal impact has increased significantly in the last century. For these reasons, significant efforts are going to be produced at the national and EU scales, either at the governance level[1] and by deploying the most advanced technologies.

Major benefits for protecting CI and enhancing the continuity of services they deliver could come from the deployment of technological systems providing access to crisis related data, allowing their monitoring and, whenever possible, the prediction of their occurrence, allowing the setup of timely preparedness and mitigation actions. A relevant role in this context could be played by Decision Support Systems (DSS). These are technological tools that can be functional to support the whole risk analysis process up to crisis management, in the preparatory and the hot phases.

A new concept of DSS should account for, and support, all phases of the risk analysis process: event forecast (where applicable/predictable), prediction of reliable and accurate damage scenarios, estimate of the impact that expected damages could have on services (in terms of reduction or loss of the services) also accounting for perturbation spreading via cascading effects, estimate of the possible consequences to citizens and to other sectors of societal life. The complete DSS workflow

[1]COUNCIL DIRECTIVE 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection.

should end up with the identification and definition of preparedness and emergency strategies that, taking into account the different phases of the expected crisis (event, damage, impact and consequence) could be adopted to reduce the impact, speed-up mitigation and healing procedures, ease the recovery phase, thus reducing as much as possible the extent, the severity and the duration of the crisis.

Such new concept of DSS can also be used as effective simulation tools to perform comprehensive stress tests on areas where the impact deriving from CI crises could be large and relevant. This activity would produce educated contingency plans based on the analysis of many (synthetic) crisis scenarios instead of being built upon (a few, when available) records of historical events. This will enhance their quality and adapt them to the effective current scenario conditions (in terms of infrastructures, assets, available technical tools, current settings of the crisis or emergency management etc.).

The EU project CIPRNet[2] has thus devoted a considerable effort to realize an novel DSS enabling to tackle the entire workflow of risk forecast of CI, from event prediction to consequences analysis.

The DSS can be supported by a large database of information collected from public and private sources. Furthermore, the DSS collects many different real-time data from the field (meteorological stations, sensor networks, meteorological radars, etc.) and forecasts from several publicly available sources (Meteorological Office, Earthquake alerts systems, etc.) producing a comprehensive assessment of the physical state of the area (urban, district, regional up to a national scale).

The availability of the geographical position (in terms of geospatial data) of the CI elements and the networks would allow, through the correlation between the physical vulnerability to natural events and the strength of expected event manifestation, to formulate an educated guess of the probability that some of the CI elements could be physically damaged by a perturbation. This analysis would thus allow to produce a "damage scenario" containing location and probability of predicted faults.

Starting from the "damage scenario", the DSS will attempt, through the analysis of appropriate simulation tools, to emulate the outages on the affected networks and, through the CI dependency information, to reproduce the effects of the cascading events propagating faults from one network to the others. This task would result in the "impact scenario", i.e. the expected profile of services unavailability over time for all the considered infrastructures.

Such data would further allow to estimating the consequences that services unavailability might produce on the different societal sectors. This is the goal of the "consequence analysis" which is meant to transform the "impact scenario" into a prediction of the social severity of the crisis, by measuring, through appropriate metrics, the consequences associated to the population, the industrial activities, the primary services (Hospitals functionality, schools, public offices, public

[2]CIPRNet, Critical Infrastructures Preparedness and Resilience research Network has been funded by EU FP7 under GA No. 312450.

transportation) and the environment (in the case when a CI crisis is associated to some type of an environmental damage).

The last step of the DSS would be the elaboration of an optimal strategies for the systems recovery by analysing possible "recovery sequences" of the different elements: the sequence "score" is evaluated in order to reduce as much as possible the social costs of the crisis.

The project CIPRNet has introduced all these elements into the DSS which has been designed and realized as one of the major outcomes of its joint technological activities. The DSS was called CIPCast. We will refer to this name in the course of this work when considering the CIPRNet DSS.

2 Design Study

In order to cast all the expected DSS properties and functions, we tried to translate the expected functionalities into a number of prescriptions, of practical issues and of technological requests to the DSS for enabling the implementation of those functions. These are the major key-words which have been translated into related functionalities of the DSS.

(1) **Prediction**. The system should provide a reliable forecast of the predictable events (e.g., heavy rainfalls, floods, etc.) with a significant anticipation, in a way to enable operators and other emergency players to set in place preparedness actions. A better choice is the setup of an incremental prediction that should start "pre-alert" periods with a large anticipation and a subsequent progressive refinement of the quality and the quantity of the prediction as the event time approaches.

(2) **Multi-hazards**. Natural and anthropic threats may damage CI. Although natural hazards (in their "intensified" strength due to climatic changes) are at forefront in public opinion, there is evidence of an increasing level of threat due to deliberate attacks, either to the physical and/or to the cyber integrity of the infrastructures. The DSS should thus be able either to analyse risks by predicting the occurrence (wherever possible) of natural threats and to provide support in the analysis of impacts due to deliberate attacks.

(3) **Dependency effects**. It is clear, nowadays, that CI form an entangled set of networks, each providing services to the others. This leads the system's control a multi-dimensional problem with multiple feedback loops propagating perturbations from one set to the others. DSS predictions should thus necessarily consider perturbation spreading due to (inter-)dependency mechanisms. This issue reflects into the need of having available the (physical or functional) "connections" data enabling to link one CI to the others.

(4) **Space and time scales**. Perturbations spread on large geographical scales. Electrical systems, for instance, can propagate a perturbation on large geographical areas in very short times. Although for some CI perturbations, and perturbations spread, occur with a very short latency, for other infrastructures

perturbation takes place on a longer time scale and, often, with a longer latency. The DSS should thus cope with multiple time scales and the geographical long-ranged perturbation spreading.

(5) **Consequences**. CI perturbations produce damage in different sectors of societal life: from perturbing the well-being of citizens, depriving them of relevant services to causing economic losses to industrial sectors, from reducing operability of lifelines (e.g., Hospitals) to damaging the environment. The DSS should also estimate which are the consequences on societal life associated to its occurrence, to provide operators and emergency managers a realistic "score" of its impact.

(6) **Data**. The realization of a system enabling a qualitative and quantitative assessment of a risk scenario does involve the availability of (often) confidential information. Geographical position of networks and CI elements, their functional data during operation times are considered confidential information by operators who restrain as much as possible their divulgation. The DSS should thus comply with these limitations and realise a trade-off for improving quality and reliability of predictions with the constraint of having access only to a restrained set of data from operators.

(7) **Support**. The presence of a multitude of data and forecast, of real time data on the scenario can be used to infer possible strategies that could be followed to reduce the impact and the consequences of the expected damages. The DSS will also provide with specific "optimization" applications enabling the solution of management problems that are normally tackled during crisis scenarios (i.e., the definition of the optimal restoration sequence when multiple elements should be repaired).

The design of CIPCast has taken into account all the issues that have been previously listed. Figure 1 shows the main functional blocks B_i of CIPCast and the relevant components i.e. the Database and the Graphic User Interface (GUI). In the

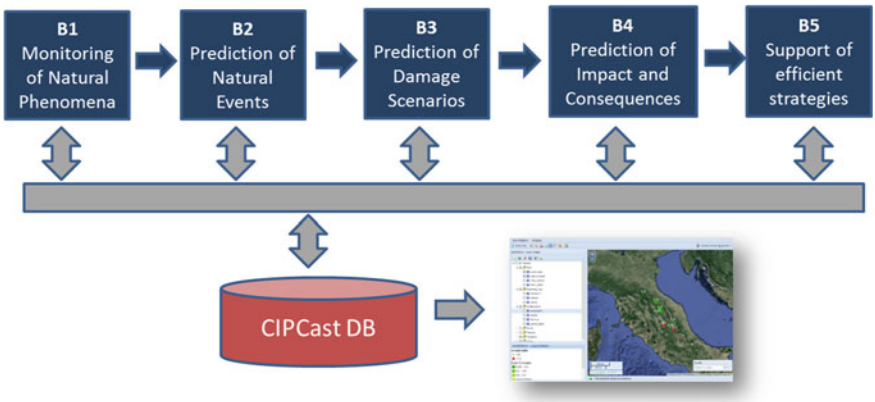


Fig. 1 Block diagram showing the main functionalities and the relevant components of CIPCast

following we will briefly describe the five functional blocks which will be better analysed in the further Sections.

Monitoring of Natural Phenomena (B1). In this block, the DSS acquires external data (real-time data, forecast) from many different sources: weather forecast and nowcasting data, seismic data, real time data coming from weather stations, hydrometer levels from water basins. These data are acquired to establish the current and predicted external conditions.

Prediction of Natural Events (B2). This block estimates the expected manifestation strength of all the predicted events. Predictions are made on different time scales: short time scale (up to 60 min from the current time), medium-long range time scale (within 48 h from the current time).

Prediction of Damage Scenarios (B3). In this block, the DSS correlates the strength of the expected manifestations with the vulnerability of the different CI elements present in the area where the events are predicted to occur, in order to estimate the probability that the manifestation could effectively damage (and, in the positive case, to what extent) the CI elements. At the end of B2 block, the DSS elaborates a "Damage Scenario" containing the information on which CI element (and to what extent) will be damaged in a specific time frame.

Prediction of Impact and Consequences (B4). This block converts the expected ***damages*** of CI elements into ***impact*** on the services the CI elements produce. This is the core of the prediction process as, in this block, the DSS transforms the expected punctual damages (to one or more CI) into a reduction (or loss) of services. To do that, CIPCast needs to deploy dependency data connecting the different CI in order to reproduce faults propagation. In addition, starting from the inoperability (or partial operability) of the different services, this block also estimates the ***consequences*** that the loss of services produces on citizens, public services, industrial activities and the environment. The ***consequences*** on each societal sector are estimated on the basis of specific metrics; a distinct "consequence score" on each societal life domain is presented separately (a unified score is not produced) in order to describe the severity of the expected crisis under many viewpoints.

Support of efficient strategies (B5). This block contains a number of applications which, taking into account the expected critical scenario, made by damages, impacts on services and weighted by the consequences estimate, will attempt to support operators and emergency managers to design and validate mitigation and healing procedures. At the current state of implementation, these supporting actions relates to:

- The identification of the optimal strategy for the restoration of the electrical distribution system after a fault, taking into account a multiple choices of optimization target functions;
- The identification of the best path which technical crews should follow (taking into account traffic conditions) to reduce restoration times;
- The optimal allocation of technical crews when the number of restoration points exceeds that of the available crews.

In the following, we will describe, in some more detail, each of the relevant elements of the DSS and the technical contents of the different blocks Bn_i.

3 Database

The geospatial Database (DB) and the related modules (GIS Server and WebGIS application) has been implemented by adopting a client-server architecture, using Free/Open Source Software (FOSS) packages. Such architecture has been properly designed to allow the interchange of geospatial data and to provide to the CIPCast users a user-friendly application, characterised by accessibility and versatility. The DB is a PostgreSQL object-relational database with PostGIS spatial database extender. PostGIS adds support for geographic objects allowing location queries to be run in SQL. The DB can be used at various levels by exploiting the potential offered by GIS tools, starting with the effective support for the operational management in the frame of the risk assessment workflow.

Data contained in the DB are classified according the following scheme:

- Input data
  - Static data
  - Dynamic data
  - Forecast
- Output data
  - Damage scenario

    Short term (<2 h)
    Medium term (>2 h and <24)
    Long term (>24 h)
  - Impact scenario

    Short term (<2 h)
    Medium term (>2 h and <24)
    Long term (>24 h)
  - Consequence analysis

    Short term (<2 h)
    Medium term (>2 h and <24)
    Long term (>24 h)

Concerning the Input data, the DB contains the following geographical information layers. Concerning with Static Data, the DB contains:

(1) Basic Geographical data (Administrative Layers, DEM, etc.);
(2) Lithology, geology, hydrography; Seismic data, earthquake parametric catalogue, seismic hazard maps and seismic micro-zoning (Florence area);

(3) Social data (census, real estate registry etc.);
(4) Hydrogeological Risk (Inventory if Italian Landslide Events, flooding risk maps, etc.);
(5) Infrastructures: (i) Electrical (transmission and distribution, Roma and Emmerich areas); (ii) Water (Roma area); (iii) Gas and oil pipelines (transmission, EU wide); (iv) Roads and railways (EU wide); (v) Telecom BTS (Roma area);
(6) CI Dependencies (Rome and Emmerich areas);
(7) Point Of Interest (POI, source: TeleAtlas);
(8) Dangerous plants (source: European Pollutant Release and Transfer Register, E-PRTR Database).

Concerning with Dynamic input data (i.e. data which are collected by field sensors, which are constantly updated), the DB contains:

(1) Weather stations (Regione Lazio);
(2) Tevere River hydrometers;
(3) Rain gauges measurements;
(4) Volcanic ashes (INGV Seviri-Modis data);
(5) Earthquakes (ISIDE).

Concerning with Forecast data, the DB contains:

(1) Weather forecast (12–24–36–48–72 h);
(2) Nowcasting (Regione Lazio, <60 min);
(3) Lightning (Central Italy, <45 min);
(4) Vehicle traffic prediction (Roma Capitale area <90 min);
(5) Marine waves and currents (Tyrrhenian Sea, Mediterranean Sea, 5 days).

The GIS Server represents the hardware/software environment that allows organizing information and making them accessible from the network. The GeoServer suite has been adopted, being a largely used open source application server, which plays a key role within the Spatial Data Infrastructure (SDI). It allows sharing and managing (by means of different access privileges) the information layers stored in the DB, according to the standards defined by the Open Geospatial Consortium (OGC), such as, for example, the Web Map Service (WMS). It also supports interoperability (e.g., reads and manages several formats of geospatial data) (Fig. 2).

The basic geospatial data and the results produced (i.e., scenarios) are stored and managed into the DB repository in order to be exploited in the different DSS blocks. To this end, the WebGIS application developed represents the natural geographical interface of CIPCast. Basic information, maps and scenarios can be visualized and queried via web, by means of standard Internet browsers and, consequently, the main results can be easily accessible to CIPCast users.

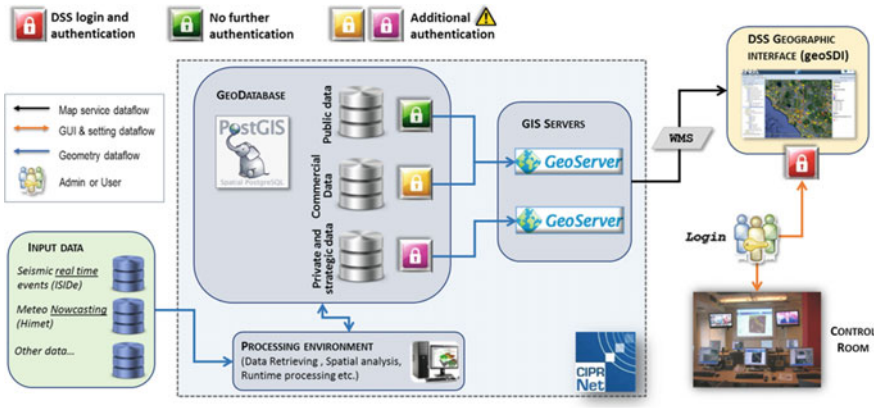


Fig. 2 Deployment diagram showing the connection among the GeoDatabase and the other DSS core components

4 Dynamic Data

In order to predict the external scenario, CIPCast has been configured to acquire external information by collecting real time data from field sensors. In particular, it acquires field data from:

(1) Seismic sensors and seismic report data;
(2) Weather stations (reporting data on rain abundance, temperature, humidity, winds, pressure etc.) and other devices that could be used to assess the specific weather conditions in a given area;
(3) Hydrometers to constantly update the level in the critical section of river basins.

Concerning seismic and earthquakes data, given as initial assumption that no real prediction can be achieved for these types of events, CIPCast receives data from the Agency committed to release this information (e.g., the National Institute of Geophysics and Volcanology INGV[3] in Italy). In the INGV official site, by accessing the Italian Seismological Instrumental and Parametric Database (ISIDE) portal,[4] information on the detected earthquakes are produced and released in real time. Upon a constant poll to the ISIDE portal, CIPCast receives the earthquakes data (within 1 min from the occurrence). Earthquake information consists of the GPS coordinates of the epicentre, its depth and the measured intensity (Richter scale). Figure 3 reports a typical snapshot of the ISIDe website.

Once earthquake data are issued, the CIPCast crawler picks them up and reports them into the synoptic chart of the DSS geographical interface (Fig. 4). The knowledge of the coordinates, the depth and the magnitude of the earthquake (basic

[3]INGV: Italian National Institute of Statistics: http://www.istat.it/en/.
[4]http://iside.rm.ingv.it/iside/standard/index.jsp?lang=en.

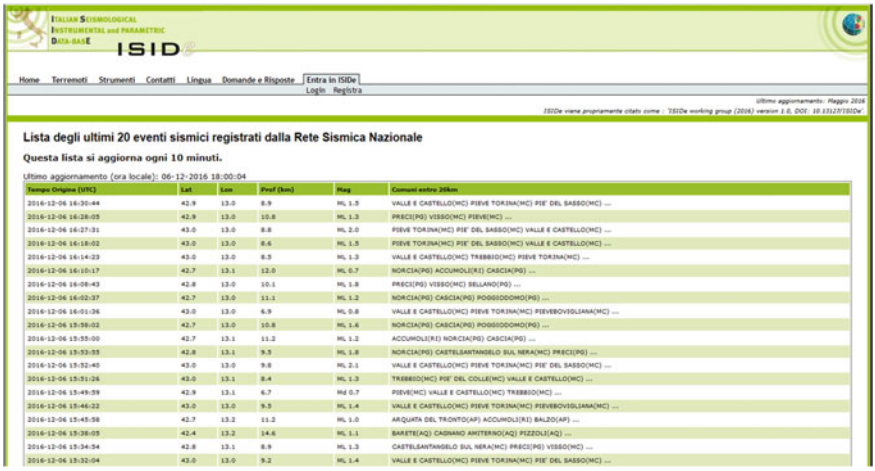


Fig. 3 Snapshot of the Italian ISIDe website providing real-time data on earthquake events occurred in the Italian territory. The portal is managed by the National Institute for Geophysics and Volcanology, INGV

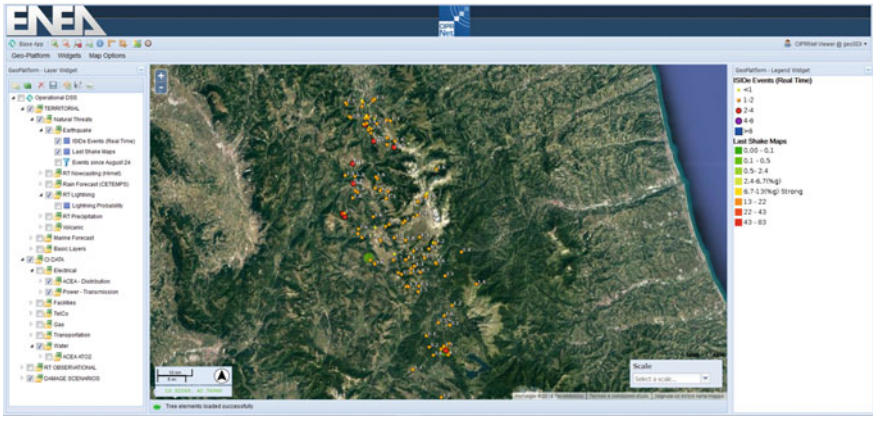


Fig. 4 ISIDe data are immediately reported into the DSS DB and visualized on the GIS web interface

earthquake's features) are not sufficient to estimate the "physical manifestations" associated to the natural event. Indeed, an earthquake creates distinct types of waves with different velocities; when reaching seismic sensors, their different travel times allow to locate the source of the hypocentre:

- **Primary waves** (P-waves) are compressional waves that are longitudinal in nature and propagate faster than other waves through the earth to arrive at seismograph stations first (hence the name "Primary");

- **Secondary waves** (S-waves) are shear waves that are transverse in nature: following an earthquake event, S-waves reach seismograph stations after the faster-moving P-waves and displace the ground perpendicular to the direction of propagation.

In the case of local, or nearby, earthquakes, the difference in the arrival times of the P and S waves can be used to determine the distance of the event. Once ISIDe operators perform their validation procedures, data of the occurred earthquakes are immediately available: based on the basic earthquake's features, CIPCast is able to convert them into a Shake Map dataset which contains, for each spatial point of a given area (as large as that involved by the physical manifestations associated to the event), the Peak Ground Acceleration (PGA) distribution induced by the seismic event.

Figure 5 shows an example of a shake map.

Other than being estimated, shake maps are usually measured by seismometers deployed all over the Italian national territory (data are first collected and then post processed by INGV) and then released by the INGV through the specific information websites. This process normally takes about 20–60 min. In order to have an earthquake shake map available in a shorter time (in order to use them for rapidly estimating expected damages), CIPCast, starting from the basic earthquake features, estimates the "predicted shake map" on the bases of empirical propagation models of shock waves in the ground and of the specific ground seismic properties (lithography and waves conductivity properties). Then, when measured shake maps are released, CIPCast perform a second damage estimate.

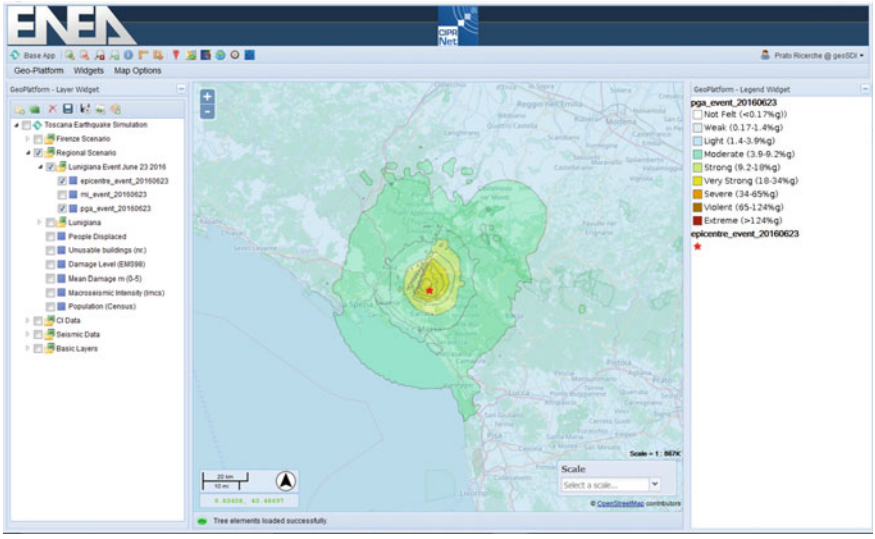


Fig. 5 The reconstructed shake map (showing the PGA estimate) for the seismic event of June 23, 2013 in the area of Lunigiana (Tuscany Region, Italy)

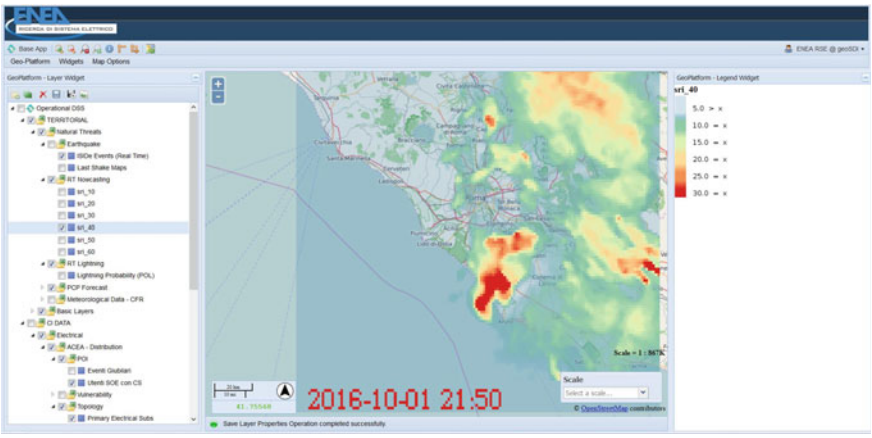


Fig. 6 Screen snapshot of the *nowcasting* prediction

Concerning weather predictions, CIPCast can deploy either medium-long term weather prediction (from 12 to 72 h) from Weather Forecasts official sources and *nowcasting* predictions (up to 60 min from the current times) provided by X-band radars. Regarding the *nowcasting* source, CIPCast receives (each 10 min) the current estimate of rain abundance and its prediction (estimated with a Local Area Model) for a time span of 60 min. The nowcasting data could be constituted either by the mosaic of several stations operating in specific points (at a national scale), mosaic which is then composed to obtain an unique picture or by a single station sweep that covers, in turn, a limited area (usually a single *nowcasting* station can cover an area of 20–30 $\times$ 10^3 km^2).

In the current setting, *nowcasting* is produced by using data of a single station (a meteorological X-band radar station) at Mount Media (in the Apennine region, nearby the city of L'Aquila) whose data covering a large fraction of Centre Italy fully comprising the Lazio Region. Data are constantly acquired and treated to extract information. From the reflectivity signals, it is possible to estimate the rain amount. These data are then post-processed in order to obtain the rain abundance prediction in a grid of 1 km of spatial resolution, for the subsequent 60 min from the current time. The resulting data (Fig. 6) are then integrated into the CIPCast DB and used to estimate the resulting damage of the CI elements.

Same data used for nowcasting prediction scan be used to provide lightning prediction. To this aim, CIPCast (every 15 min.) acquires lightning probability data related to the next 45 min and visualises them on the GIS interface. The data source computes the lightning probability using various indices of the Weather Research and Forecasting model.[5] In the current setting, the monitored area for lightning probability covers a large fraction of centre Italy fully comprising the Lazio Region. Figure 7 shows an example of a lightning probability map. Following the

[5]http://www.wrf-model.org/index.php.

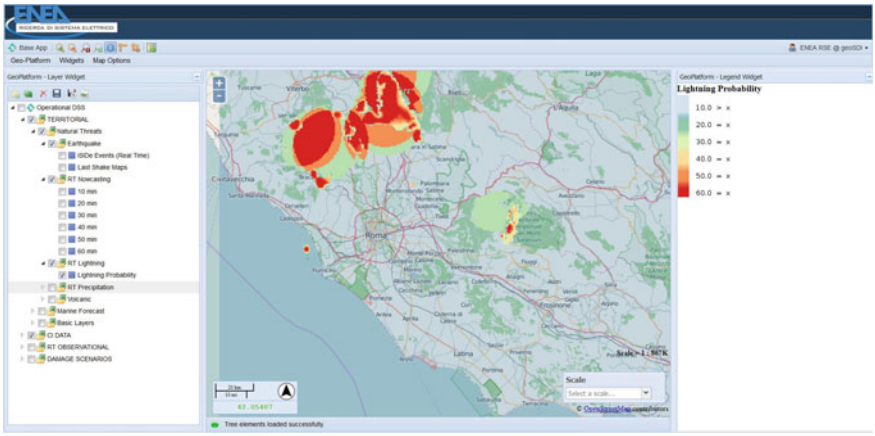


Fig. 7 A snapshot of the Lightning Probability map

guidelines for lightning probability greater the 60% the CI operators should monitor their infrastructures and in particular those components that are vulnerable to lightning events.

To sum up, there are two events prediction based on:

- ***Nowcasting and Lightning*** for the short-term where the accessed and achieved data are sufficient to estimate damage scenarios and no further data elaboration is made in CIPCast;
- ***ECMWF data*** (Fig. 8) for the medium-long term weather prediction down-scaled through a LAM to create a specific map reporting the spatial distribution (approximately, 5 km × 5 km) of the precipitation rate of rainfall forecasts (mm/h). Forecasts are produced and available for a time span from 0 to 48 h (6-h intermediate steps), starting from 0:00 a.m.—UTC of each day. Such data are continuously and automatically retrieved from a specific web-service, in NetCDF[6] format, and directly stored into the CIPCast DB, in order to exploit them within the DSS application (Fig. 9).

At the end, CIPCast produces a comprehensive description of the current (and forecast) scenario, by providing a map of all the physical manifestations related to the predicted (and/or the on-going) natural events with their magnitude (each expressed in a specific strength metrics).

These information are then transferred to the further building block, where event' manifestations strength are "transformed" into expected damages to the CI elements.

[6]http://www.unidata.ucar.edu/software/netcdf/.

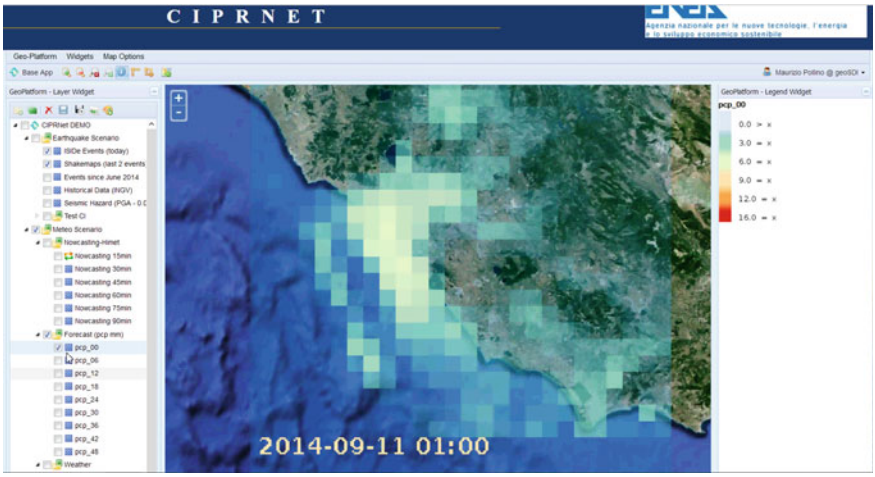


Fig. 8 Precipitation rate forecast example map (Himet processing of ECMWF data)

5 Damage Scenario Builder

Once a reliable awareness of field data is achieved, also supported by the results of the different forecast systems, CIPCast attempts to build a **Damage Scenario** consisting of the list of all the identified CI elements expecting to be damaged by the expected natural phenomena with the predicted strength.

The first action is to cast the external prediction into a *Threat Strength Matrix*, containing the strength of the predicted physical manifestations associated to the expected natural events. Each natural hazard, in fact, manifests in a different way (winds with physical pressure exerted on the structural elements, heat waves with temperature raise etc.). If we normalize the value (expressed in the appropriate unit of measure) of the strength of each perturbation manifestation in an arbitrary scale from 1 to 5, we could define, for each geographical position, a *Threat Strength Matrix* describing the intensity of the associated manifestations.

Table 1 shows the Threat Strength Matrix $\boldsymbol{S}$ associated to a given geographical position (x, y). Each row contains the expected strength of the manifestation associated to the natural event.

Whereas geographical points will be characterized by the strength of the expected natural manifestation (cast into the Threat Strength Matrix), each CI element (located in some geographical position) will be characterized by a *Vulnerability Matrix* $\boldsymbol{V}$, which identifies, for each perturbation manifestation, the limiting strength that the element could sustain before being damaged. The $\boldsymbol{V}$ Matrix will then have same entries of the Threat Strength Matrix; it provides, in turn, the limiting grade of the perturbation strength that the CI element can sustain before failure. If, thus, the V_{ij} element of the matrix will be different to zero, all

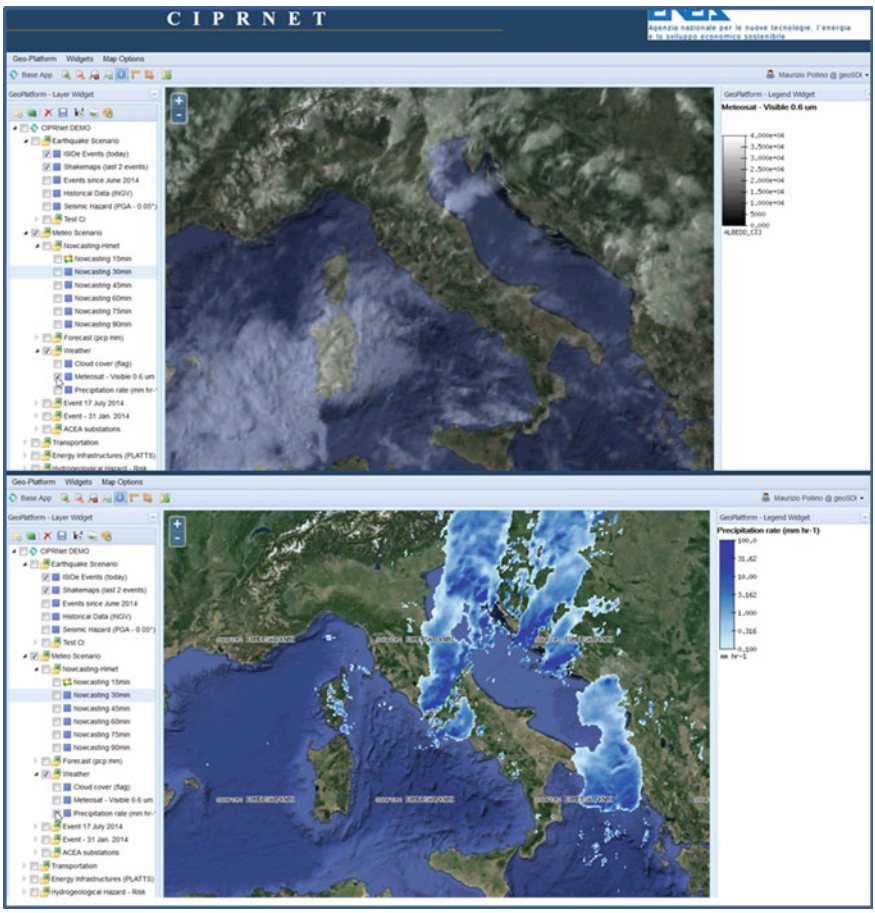


Fig. 9 Cloud cover and precipitation rate map views (Eumetsat/ECMWF)

other elements $V_{i(j+k)}$ will be not vanishing: if V_{ij} strength perturbs (or damages) the CI elements, all larger strengths, a fortiori, will do.

Table 2 shows the Vulnerability Matrix $\boldsymbol{V}$ associated to a specific CI element. Each row contains the perturbation extent that a manifestation of a specific grade is expected to produce on the element. In general terms, the extent of physical damage D produced by a threat manifestations S on the CI element having a vulnerability matrix V will be given by

$$\mathrm{D} = \max\left\{\mathrm{s_{ij}} \cdot \mathrm{v_{ij}}\right\}$$

where operation indicated with $\cdot$ is the ordinary product between the values $\mathrm{s_{ij}}, \mathrm{v_{ij}} \in \mathbb{R}$ of the two matrices. If $\mathrm{D} = 0$ the CI element will not be harmed by the perturbation(s), while if $\mathrm{D} \neq 0$ it will be damaged up to a certain extent $(0 < D \leq 1)$.

Table 1 Threat strength matrix

Threat name	Threat grade					
	1	2	3	4	5	Associated physical manifestation
Earthquake	0	0	1	0	0	PGA (peak ground acceleration)
Strong wind	0	1	0	0	0	Wind speed (pressure)
Lightening	0	0	0	0	0	Probability times voltage
Heavy snowfall	0	0	0	0	0	Weight (pressure)
Ice	0	0	0	0	0	Weight (pressure)
Landslide	0	0	0	0	0	Stress
Flash flood	0	0	0	0	0	Water level
Flooding	0	0	0	0	0	Water level
Mud flows	0	0	0	0	0	Weight (pressure)
Debris avalanches	0	0	0	0	0	Weight (pressure)
Heavy rain	0	0	0	0	0	Water level
Strom surge	0	0	0	0	0	Water level
…	0	0	0	0	0	

In the example, the event will consist in an earthquake (on intensity 3 in an earthquake magnitude scale 1–5) with an associated strong wind (of magnitude 2 in the 1–5 wind scale)

Table 2 Vulnerability matrix

Threat name	Vulnerability grade				
	1	2	3	4	5
Earthquake	0	0	**0.5**	**1**	**1**
Strong wind	0	**1**	**1**	**1**	**1**
Lightening	0	0	0	**1**	**1**
Heavy snowfall	0	0	0	0	**1**
Ice	0	0	0	0	**1**
Landslide	0	0	0	0	0
Flash flood	0	0	0	0	0
Flooding	0	0	0	**1**	**1**
Mud flows	0	0	0	0	0
Debris avalanches	0	0	0	0	0
Heavy rain	0	0	0	0	0
Strom surge	0	0	0	0	0
…	0	0	0	0	0

In the example the CI element whose V matrix is displayed would be partially damaged by a grade 3 earthquake and totally destroyed by larger magnitude events, it would be destroyed by winds of magnitude ≥ 2, by lightning ≥ 4, by floodings ≥ 4

Figure 10 reports the WebGIS interface of CIPCast, containing various geospatial layers and the information on the expected Damage Scenario. CI elements are classified on the bases of the prediction time of their outage (red elements predicted to be failed in 15 min, darker-coloured elements at progressively longer times).

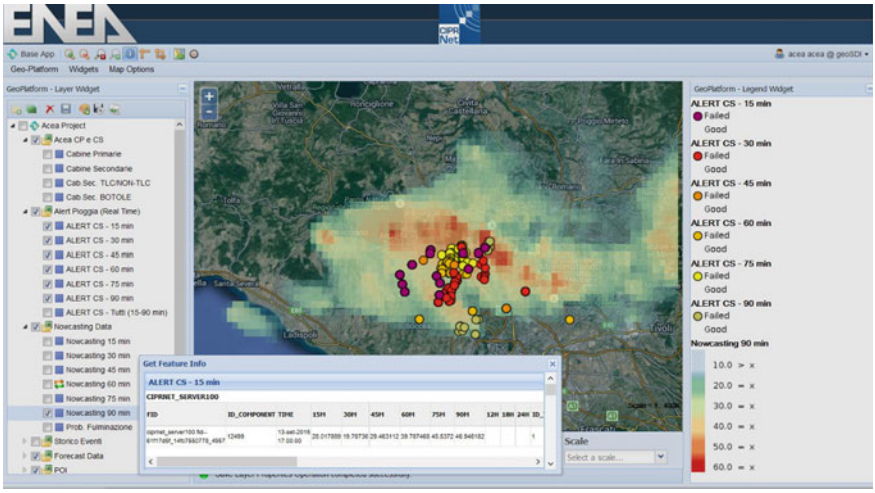


Fig. 10 Cloud cover and precipitation rate map views (Eumetsat/ECMWF)

6 Impact Scenario

The **Impact Scenario** takes the Damage Scenario as an input from the B3 block. This contains, for a given time frame, the set of the CI elements that are predicted to fail.

CIPCast, at this stage, run an application called RecSIM (Reconfiguration actions SIMulation in power grids [1, 2]) a simulator that, starting from the identification of the behaviour of the electrical-telecommunication system upon the outage of one (or more) of their components, spreads the perturbation also to other CI infrastructures. This approximation (that is similar to an adiabatic approximation while treating perturbations in quantum theory) is somehow legitimated by the fact that the response of the electro-telecom systems occurs with characteristic times much smaller than those of the other systems. In this respect, CIPCast first deals with fast degrees of freedom (electrical and telecommunication networks response) and then propagates the perturbation to other degrees of freedom (i.e. the other CI networks).

7 RecSIM

RecSIM is a discrete-time event-based Java simulator designed to emulate the network management procedures by an electrical distribution system operator and to estimate the evolution of the electric network. Although the implemented

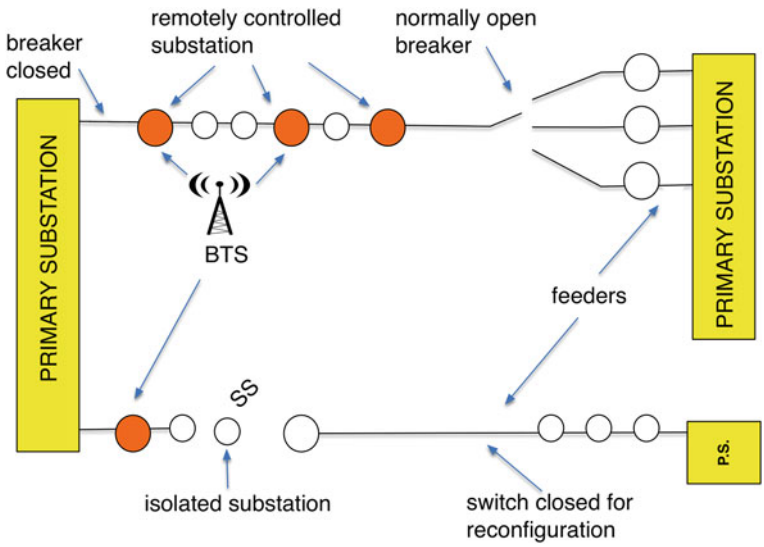


Fig. 11 Modelled components of the electric grid

operations are related to a specific electrical operator,[7] these procedures should be thought as general; they are, in fact, adopted by other operators for the reasons that they take into account only the basic functioning mechanisms of a switched and controllable electrical network. RecSIM assumes an electrical distribution model where each electrical node (a primary or a secondary substation) may feed a telecommunication device, called Base Transceiver Station (BTS) that, in turn, ensures remote control capability to the electrical grid.

Figure 11 sketches the main ingredients (i.e. the elements) needed to design an electro-telco grid used for the RecSIM modelling and simulation.

- **Primary Substations (PS)** (containing HV → MV transformers);
- **Feeders**. Each PS supplies a number of MV feeders that hold the secondary substations;
- **Secondary Substations (SS)** (MV → LV transformers). Some of them are remotely controlled (in the Rome distribution network about 50% of the SS are remotely controlled);
- **Switches**. The terminal SS of each feeder ends with a switch. The network exhibits a "normal configuration" when all the switches of the terminal SS are open. In general, this configuration represents the optimal configuration for the electric operator and he/she usually will aim to manage the network in this configuration. Anyway, due to failures/maintenance this is not always possible.

[7]ACEA Distribuzione SpA, the major electrical distribution operator in the area of Regione Lazio (Italy).

By closing the switches, it is possible to energize the SS belonging to one feeder through other PS belonging to other feeders thus changing the normal configuration.

In a real electrical distribution network, as soon as a failure occurs, some actions are performed by specific automatic control systems. For instance, the protection systems open some switches in order to avoid the propagation of the failure as well as the damage of electrical components (e.g., electrical feeders). Within a delay of the order of milliseconds, there is usually an automatic reaction of the network to a failure (of a component or along the lines). This automatic reaction is instantaneous, so if the failure happens at time t_0 all actions performed by the protection systems will be performed at t_0. Soon after the perception of the fault, the electric operator will be notified alarms through the SCADA system and will try to isolate the failures as well as to reconfigure the electrical network to provide electrical power to those substations that might be involved in the blackout. The automatic reaction produces the blackout of an entire feeder containing electrical substations (from a few up to some tens, in the worst case). At this stage, the electric operator can usually perform one (or more) of the following actions:

(1) To "remotely" perform failure isolation and reconfiguration actions of the network by sending commands to the remotely controlled substations;
(2) To dispatch Emergency crews (usually deployed in the field) to "manually" perform failure isolation and reconfiguration actions of the network;
(3) To "deliver" Power Generators (usually located in deposits) to feed isolated substations for the time being (from some hours to some days) required to repair the failure.

In order to make use of the remote control capability, the operator should first verify the reachability of the remotely controlled devices (e.g., Remote Terminal Units or Programmable Logic Controllers) deployed in the substations and required to perform the opening and closure of breakers. At this stage, dependency mechanisms can play a crucial role. Indeed, the faulted electrical feeders can inhibit the power supply to some BTS. Considering the strong interdependency among electrical SS and telecommunication BTS, damages occurring in one (or both) network can cause disruptions that hold in the short time scale (from a few minutes up to some hours) leaving people without power and/or mobile communication services.

As mentioned, if remote control is available, the electric operator will send commands to close switches to re-energize part of the network. These actions usually take some minutes to be completed (e.g., 3–5 min). In case the SCADA system is not working or the devices cannot be remotely controlled, the electric operator must dispatch an emergency crew to manually perform reconfiguration action. In this case, emergency crew actions may require about 1 h to be completed (depending on the state of urban traffic). However, there are cases where no actions are available to re-energize part of the network. In such cases, the only possible option is to send one (or more) Power Generator to supply the Low Voltage (LV) line(s) usually supplied by electrical substations. The action of displacing a

Power Generator and re-supplying a single Medium Voltage (MV) line may require some hours to be completed.

RecSIM takes into account all these procedures and the number of emergency crews and power generators available to the electric operator to estimate the evolution of the networks.

In order to use RecSIM to reproduce a generic electric network the following information about the electric network topology are required:

- The connecting feeders for each PS;
- The ordered sequence of SS connected to the different feeders;
- The position of the terminal switches that can enable any network reconfiguration;
- The set of SS that can be connected (closing the switches) to each terminal SS to implement a contingency to reenergize some SS after some failures occur.
- The remotely controlled SS;
- The set of BTS providing connectivity to the remotely controlled SS;
- The set of SS feeding the BTS;
- The number and the initial position of the emergency crews and power generators.

RecSIM can, on the basis of the available resources, optimize the sequence of restoration operations to be followed in order to produce the least consequences to citizens and/or to minimize the overall outage time. RecSIM allows the operator to autonomously design a strategy given by an ordered sequence of operations to restore the networks. In the latter, no optimization procedures are involved.

Operators are committed to release their services with a predefined Quality Level expressed, for instance, by using the Service Continuity Indicator measured in terms of "kilo-minutes of outages (***kmin***)":

$$kmin = \sum_{k=1}^{N} u_k T_k$$

where ***kmin*** is the sum of the products between the number of minutes of outages times T_k for each k-th SS and u_k is the number of electric customers fed by the k-th SS considered for the interval time of interest.

Other than the number of ***kmin*** expected before the crisis end, additional optimization functions could be used in the optimization strategy. CIPCast, in its Consequences Analysis module (see next section), can produce a more "societal-oriented" optimization function which takes into account the reduction of well-being of different societal sectors (Citizens, Economic Activities, Public Services etc.). RecSIM allows to choose among different optimisation functions before launching the optimisation strategy.

Figure 12 shows the Impact Scenario for a limited area of the electrical grid of Rome where it is possible to observe the SS affected by an electric outage.

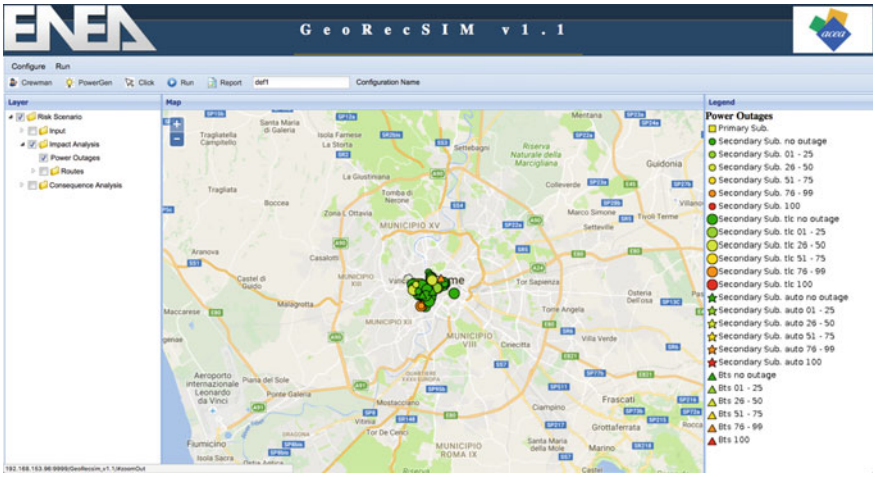


Fig. 12 Snapshot of RecSIM GUI (colours from *green* to *yellow* denote increasing expected outage times over an interval of interest)

Figure 13, in turn, indicates the best possible route to be followed by a technical crew to reach the site where a restoration operation should be executed. The path could also be determined as a function of the current or predicted state of urban traffic, by considering, in the shortest path algorithm, the different times needed to tread the different arcs of the city street graph. CIPCast is also connected to an application which, based on historical traffic data and the current real time data, can predict the state of traffic in the next 90 min. Traffic prediction can improve the quality of the identification of the shortest path (Fig. 13) to be suggested to the

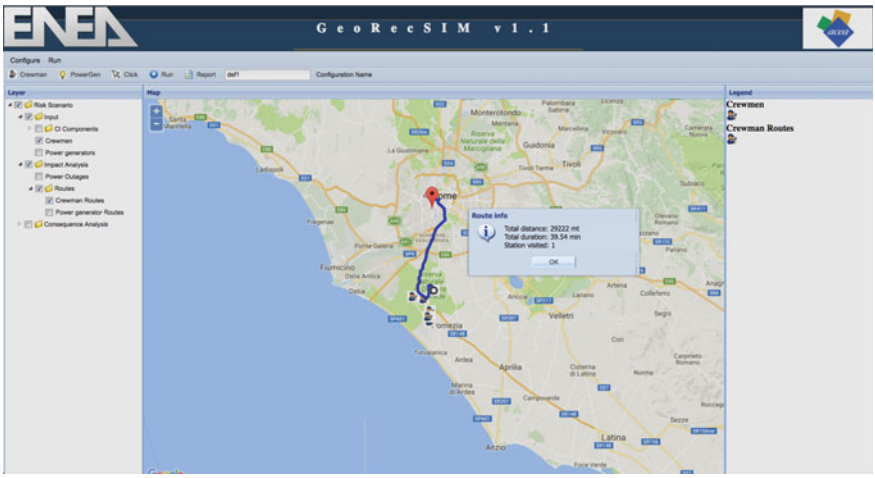


Fig. 13 Route executed by an emergency crew to isolate a faulted substation

technical crew to move toward the site where the technical intervention should be produced.

8 Consequence Analysis

After having defined the *damages* produced by a natural event or by a man-made incident and recognised the *impacts* that those *damages* might produce on the functioning of CI, the CIPCast system attempts to estimate, as the final step, the *consequences* produced on society by the events striking a given area.

As the Service Continuity indicator (***kmin***) is one of the major KPI of an electrical Utility, CIPCast performs the estimate of such an indicator. The service standard requested to the operator by Public Authorities (expressed in terms of minutes of LT outages per year) takes in some way a social meaning as this value represents a socially acceptable duration of loss of a relevant service as electrical power and users are retained as equally important. Moreover, CIPCast attempts to estimate the possible consequences of a crisis scenario taking into account other metrics weighting losses that any outage might create to the different societal sectors.

It is worth noting that although we mostly refer to natural events, the same Consequence Analysis model could be usefully applied to any event (also of anthropic origin) on CI which produces an impact on their services.

In order to define the scope of the Consequence Analysis (CA hereafter) it is useful to point out that, in general, a natural event produces two types of *consequences*:

- *direct consequences* encompassing all the effects due to the direct damages produced by the event (disruptions, contingencies etc.);
- *indirect consequences* considering the loss of the well-being produced by the unavailability of Primary Services (PS) supplied by CI, which are
  - electricity (provided by the electrical system, i.e. transmission and distribution grids)
  - telecommunication (voice and data communication types)
  - water (drinkable water)
  - gas (and other energetic products)
  - mobility (unavailability of public transports induced by other PS outages).

Taking an earthquake as a case study, for example, we will ascribe to the *direct consequences* the number of casualties (due to buildings collapse following the earthquake) and the economic cost needed to restore/retrofit (or rebuild) the damaged buildings. In turn, we attribute to *indirect consequences* the social and economic costs inflicted to the society by the unavailability (or partial availability) of the primary services (electricity, telecommunications, drinkable water, mobility etc.). Thus *damages* on CI elements produce *impacts* on their services which inflict

consequences (of the class of indirect consequences) to societal life. Although CIPCast is able to consider both types of consequences, a major effort has been carried out to set up a model able to estimate the *indirect consequences*.

The first step of the Consequence Analysis has been the identification of the sectors of the societal life to be considered, in order to fully describe the *indirect consequences* inflicted by a crisis of CI services to those sectors and, for a given sector, to each sector's element as well as to identify—for each sector element—the "consequence metric" C_i which better measures the extent of the *consequences*.

A thorough analysis has allowed to focus on the most vulnerable sectors prone to be damaged (in terms of well-being reduction, ***Wealth*** hereafter) by the unavailability (or a partial availability) of PS supplied by CI:

- Sector 1 is about Citizens and the consequence metric C_1 provides a measure on the number of Citizens involved and the extent of the reduction of the well-being caused by the PS outage;
- Sector 2 is about the economic activities and the consequence metric C_2 takes into account the amount of the GDP lost due to PS unavailability;
- Sector 3 is about Public activities and services such as schools, hospitals, public offices. The consequence metric C_3 gives indication about the number of affected activities and/or their reduction of capabilities (PS outages or reduction could lead to a reduction in the number of healed patients per hour in a hospital, while partial blackouts could reduce the number of potential users of public transportations etc.)
- Sector 4 is about the Environment and the consequence metric C_4 is expected to give clues about (long term and short term) environmental damages (dimension of polluted areas, expected costs for reclaiming etc.).

The CA model refers to the identification (and a quantitative estimate) of an *expected* Wealth for each Sector element and the way to estimate its reduction upon loss (or reduction) of the benefits associated to the PS availability.

We can define the **Wealth W(t, $\mathbf{t_{ij}}$)** of a societal Sector element t_{ij} as a function of the available Services Q_k at time **t** as follows:

$$W(t, t_{ij}) = M(t_{ij}) \sum_{k=1}^{N_k} r_k(t_{ij}) Q_k(t) \quad (1)$$

Wealth of a societal Sector element

where:

- N_k is the total number of the considered Services which contribute to Wealth (electricity, telecommunication, gas, water and mobility);
- M_{ij} is the Wealth metric (for example, number of people who can access and need to rely on the Services, or the expected/projected turnout in the economy sector j during the time period T).
- $r_k(t_{ij})$ is the relevance of the k-th Service for the achievement of the maximum level of the Wealth quantity M for a given element of Criteria.

- Q_k is the availability level of Service k (if $Q_k = 0$ the Service is fully unavailable). Q_k depends explicitly on time and describes the pattern followed by the outage of the k-th Service during the time course of the Crisis. The function $Q_k(t)$ is the outcome of the Impact Analysis.

The elements $r_k(t_{ij})$ are the measure of the relevance of the Service k for the Wealth achievement in a given Sector element. For this reason, they will be identified as Service Access Wealth (SAW) indices. They may be different from each other: a Sector element can be more vulnerable to the absence of a given PS and, thus, its Wealth most affected if that specific PS would fail. We then consider a closure relation, such as

$$\sum_{k=1}^{N_k} r_k(t_{ij}) = 1 \quad \forall\, t_{ij} \tag{2}$$

Closure relation of SAW indices

It is worth noticing that a more accurate analysis would imply the use of a residual term ($r_k(t_{ij})$ with $k = N_k + 1$). This further term would account for the fact that for many societal Sectors, the eventual loss of all services would not imply a total loss of well-being. In other words, the loss of all Services, as a whole, will reduce of a different amount the Wealth of the different societal Sectors. Thus we would rewrite the closure relation in Eq. 2 by adding a further term which we would call "well-being residue".

$$\sum_{k=1}^{N_k} r_k(t_{ij}) + r_{res}(t_{ij}) = 1 \quad \forall\, t_{ij} \tag{3}$$

A more complete closure relation of SAW indices

In a first approximation, $r_k(t_{ij})$ are considered as time-independent, although their variation in time could be properly assumed (such as, e.g., the loss of a PS for an economic activity could be less detrimental during the night hours when production is stopped). The unitary closure constraint could be kept fixed even in the case of time variation of the SAW indices. For a discussion on the time-dependence of SAW indices see Appendix 1.

If $Q_k(t)$ are all unitary, Wealth W is as expected. If, in turn, some $Q_k(t)$ will be not unitary (or even vanishing) for some time during a period T, say, Wealth is expected to be reduced accordingly. Thus we can identify as Consequence C for a given Sector element in the time T of crisis duration the difference between the expected and the achieved Wealth

$$C(t_{ij}, T) = M(t_{ij})T\left[1 - \sum_{k=1}^{N_k} r_k(t_{ij}) \int_0^T Q_k(t)dt - r_{res}(t_{ij})\right] \tag{4}$$

Consequence C on the Sector element t_{ij}

It's worth pointing out that

Table 3 List of all considered sectors elements for the CA analysis

Sector	Elements			
Citizens	Age t > 65	Age 0 < t < 5	Age 18 < t < 64	People with disabilities
Economic activities	Primary sector	Secondary sector	Service sector	
Public services	Schools	Hospital	Public transportation	Safety and security
Environment	Land	Sea	Water basins	

$$\begin{array}{ll} C\left(t_{ij},T\right)=0 & \text{if } Q_k(t)=1 \text{ for all } k \text{ and for all } t\in[0,T] \\ C\left(t_{ij},T\right)=M\left(t_{ij}\right)T\left[1-r_{res}\left(t_{ij}\right)\right] & \text{if } Q_k(t)=0 \text{ forall } k \text{ and for all } t\in[0,T] \end{array}$$

Extreme Consequence values

(5)

The residue term represents the part of the Wealth which could not be attributed to the deployment of the Primary Services; if it is non-vanishing, it inhibits the possibility that the Consequence C becomes as large as the total Wealth (see Eq. 5).

The CA model requires the identification of two sets of data: the Wealth metric $M(t_{ij})$ and the SAW indices $r_k(t_{ij})$ for all the Sector elements t_{ij}. The Primary Services (PS) availability functions $Q_k(t)$ are, in turn, the output of the Impact module of the system. Before considering the SAW indices estimate procedure, it is worth identifying the Sector elements that the model will consider for a complete assessment of societal consequences after a CI crisis (Table 3).

9 SAW Indices Estimate

The evaluation of the SAW indices for the different Sector elements may require the use of different approaches (and data sources). Information about Citizens are provided by the National Institutes of Statistics (in Italy, ISTAT[8]) and could be refined by data provided by service Utilities. Information on economic sectors could be, in turn, obtained at the Chambers of Commerce or from trade category Associations or elicited by specific historical or ad hoc surveys.

To elicit the SAW indices for each Sector element, multiple data sources may be used, either alternatively or jointly.

It is clear that, being societal Sectors different from each other, the meaning of the term "relevance" (identifying the impact that the unavailability of a specific PS would have on each Sector) will be very different: we will span from discomfort to economic losses or to the threat of physical integrity. The chosen metrics $M(t_{ij})$

[8]Italian National Institute of Statistics (http://www.istat.it/en/about-istat).

Table 4 Association of the relevance concept to each of the CA sectors

Sector	Wealth metrics	Concept used to identify SAW indices
Citizens	# Affected people	Level of usage of each PS in the daily life; prioritization according to safety and discomfort level
Economic activities	Turnout loss	PS role in allowing the achievement of the production goals
Public services	Service capability	PS role in making the services available to citizens and stakeholders
Environment	Areas affected	

Table 5 Type of data used for the identification of SAW indices for a given sector

Sector	Wealth metrics	Data used to determine SAW indices
Citizens	# Affected people	Hours of usage and priority of the different PS
Economic activities	Turnout loss	Yearly expenditures for having available the different PS
Public services	Service capability	Elicitation with stakeholders and Public Services operators
Environment	Areas affected	Elicitation with stakeholders and Environmental operators

expressing the Wealth for a given Sector element will account for these issues. When $M(t_{ij})$ is an economic value (the production value for a given plant, for instance), the term "relevance" (and the associated SAW indices) will express the importance of a specific PS to allow the plant to achieve the planned production value. There could be, obviously, activities whose production is more related to the availability of electrical power (i.e. manufacturing), while in other cases it is more related to availability of telecommunications (i.e. digital commerce). This difference will reflect into the values of the corresponding SAW indices.

The following tables (Tables 4 and 5) report the relationships between the term "relevance" and the different Sector's elements through the indication of the related Wealth metrics $M(t_{ij})$.

In the following, we will describe the way to approach the SAW indices identification from available data for two different Sectors: Citizens and Economic Activities. In the first case, a complete assessment of the indices will be provided, where the attempt to estimate time-dependency of relations will also be done.

9.1 SAW Indices Estimate for the Citizens Sector

Table 6 summarises the indices to be calculated for the Sector "**Citizens**" **and its elements**.

Table 6 SAW matrix for the four different Elements of the Citizens Sector

Sector elements	Primary services (PS)				
	Electricity	Telecom	Water	Gas	Mobility
Citizens 65+ t_{11}	$r_1(t_{11})$	$r_2(t_{11})$	$r_3(t_{11})$	$r_4(t_{11})$	$r_5(t_{11})$
Citizens 0–5 t_{12}	$r_1(t_{12})$	$r_2(t_{12})$	$r_3(t_{12})$	$r_4(t_{12})$	$r_5(t_{12})$
Citizens with disabilities t_{13}	$r_1(t_{13})$	$r_2(t_{13})$	$r_3(t_{13})$	$r_4(t_{13})$	$r_5(t_{13})$
Citizens 18–64 t_{14}	$r_1(t_{14})$	$r_2(t_{14})$	$r_3(t_{14})$	$r_4(t_{14})$	$r_5(t_{14})$

First of all, it is worth reporting one of our main findings which is that inferring the relevance of services for different Sector elements from the analysis of the family budget devoted (by each Sector element) to the access to a specific PS is not accurate enough because it is very difficult to take into account important factors such as family income, different technologies and different service pricing (we are interested in the usage and its relevance, not in the expenditure), although such analysis can give a rough initial clue about the relevance ratio among elements of the same Sector.

In fact, we found that a more accurate analysis takes into account service usage (time and criticality) and—as far as it concerns the Electricity usage from different customers—interesting hints can be found in the measurement campaigns [3–5].

More in details, in [5] the authors defined as relevant—for the Italian case—the following power-enabled "services" ordered by priority: lighting, refrigerator and freezer, oven, TV, microwave, washing machine, dish washer, drier, iron. They also included in their analysis cooking facilities as they included kitchen with induction as an electrical load: its priority is lower than the fridge and higher than the oven.

The rationale behind the sequence above is the following. Lighting is the first service in order of importance because of the personal safety which would be affected by its absence and the fact that no activity is possible in the absence of illumination. The refrigerator and the freezer were placed nearly at the same priority level as their continued operation is essential for the proper storage of food which, should remain at room temperature for too long without being consumed, lose their health and should be thrown away. Next primary service is the kitchen, less important just than a refrigerator and freezer also because its massive use is limited at mealtimes, when usually no other parallel activities are in place. As it has been said before, in Italy kitchen is usually gas powered but priority considerations are still valid.

Next appliances alias services in our priority list are electric oven and TV. This is because, based on the frequency of use and perceived importance of the service provided, they can be seen as equally important.

The microwave was placed behind the TV as it does not really offers an essential service: in Italy, it is actually a substitute for traditional stoves, typically used to heat the food in a short time and rarely to cook.

Other appliances like washing machine, dishwasher and dryer were considered less important than, for example, the microwave because of the duration of use. According to the authors of [5] in fact, considering that the microwave is usually

used for short periods, it makes more sense—with respect to the perception of comfort—to interrupt a wash cycle rather than having to wait maybe an hour or more to warm a cup of tea.

Behind them it has been placed the iron, since according to the logical order of use is the latest after the dryer but still less urgent than a cycle of the dishwasher.

Other appliances are not included because they offer services that are not necessities but are related mostly to individual needs. These include hair dryer, vacuum cleaner but also PC and videogames.

Taking into account the above suggestions and making hypothesis about usage for the different Sectors when they are at home, we calculated for the different groups different profiles (see Appendix) that are coherent with independent studies and measurement campaign, for example [3, 4].

Backed up by the good matching with experimental results, we applied the same methodology to water and gas and, as we didn't find similar independent studies assessing the priority of different gas—an water-enabled services, we built our profiles based on the knowledge of the typical Italian household. More in details, we considered the stove, the water heating and the heater as gas-enabled services and drinking water, domestic water and waste water as water-enabled services.

Resulting profiles are shown in Appendix.

About the SAW indices related to Telco services, we considered mobile, land-line and Internet. As far as their usage in time is concerned, different customer profiles have been taken into account (for example, employed people will not stay at home between 8 a.m. and 5 p.m.; for them, a home telco outage would not have a significant impact). On the other hand, as far as the priority is concerned, ISTAT has gathered a "microdata" set reporting the answers to a specific survey with 760 questions of 20,000 households. Questions are on different subjects and 50 of them are related to the usage of the telco services and their relevance for different groups. Summing up the number of different services each group uses very often we found the required indices.

At the end, the SAW indices for the different Citizens Sector elements are reported in Table 7. To make the consequence calculation easier they are time-independent although the carried out analysis is definitely time-depended. The conversion has been done by summing up all the usages in all the timestamps and normalizing to the highest value.

Table 7 SAWI matrix for the elements of the citizens sector

Sector elements	PS				
	Electricity	Telecom	Water	Gas	Residue
Citizens 65+ t_{11}	0.398	0.126	0.343	0.134	0
Citizens 0–5 t_{12}	0.234	0	0.181	0.095	0.49
Citizens 18–64 t_{14}	0.288	0.145	0.212	0.097	0.258

Table 8 SAW indices for the three different elements of the economy criterion

CA criteria	Services				
	Electricity	Telecom	Water	Gas	Mobility
Primary t_{31}	$r_1(t_{31})$	$r_2(t_{31})$	$r_3(t_{31})$	$r_4(t_{31})$	$r_5(t_{31})$
Secondary t_{32}	$r_1(t_{32})$	$r_2(t_{32})$	$r_3(t_{32})$	$r_4(t_{32})$	$r_5(t_{32})$
Tertiary t_{33}	$r_1(t_{33})$	$r_2(t_{33})$	$r_3(t_{33})$	$r_4(t_{33})$	$r_5(t_{33})$

Please note that the analysis assumes a "normal" situation to assess the priorities but we are aware that priorities during an emergency could change. As an example, charging batteries for mobile phones—according to what happened in the 2002 Flooding in Germany—could be a separately profiled function and could be high in rank. Anyway, assessing the priorities during an emergency strongly depends on the type of crisis and on the specific scenario.

9.2 SAW Indices Estimate for the Economic Activities Sector

As far as it concerns the **Economy Activities Sector**, Table 8 summarizes the SAW indices to be calculated for the Economic Activities Sector elements (Primary, Secondary and Tertiary activity areas) for the PS.

As previously stated, in the Economic Activities Sector elements the relevance of each PS has been related to the effects that their unavailability would have in terms of economic losses, i.e. relevant is all that is needed to perform the related production (of goods or services).

Thus the Wealth metrics is the turnover produced (in a given amount of time) and the Consequences are measured in terms of turnover lost. For this reason, an accurate and reliable estimate of the value of $M(t_{ij})$—i.e. the expected turnover produced per time unit—is a relevant quantity to be determined beforehand.

For achieving these data, still keeping a statistical approach, we have used *the input-output matrices* [6]. These data are usually released by the National Institute of Statistics and acknowledged in the national accounts of many countries.

The input-output tables are $n \times n$ matrices representing the mutual relations between the various economical activities, showing which and how goods and services produced (output) by each activity are used by others as inputs in their production processes. In Appendix 2, we elaborate on the specific case of the definition of SAW indices for the economic sectors.

10 Other Operation Modes and Future Work

Other than releasing "real time" prediction (i.e. in a 24/7 operational mode) by collecting external data from forecasts and field sensors, CIPCast can also be used in "off-line" mode. In this mode of operations, real external scenario could be

substituted by synthetic events whose main manifestations are somehow introduced in the B1 block as if they were real. In this respect CIPCast can simulate synthetic events (it can currently simulate synthetic earthquakes and abundant rainfalls in specific area). This operation mode is called “Event Simulator”. This mode is meant to be used by operators and other Public Authorities for producing stress tests of their systems and/or to study contingency plans adapted to expected (or risky) events. This could enhance the ability of designing preparedness measures and contingency plans, other than revealing (upon quantitative analysis) infrastructural elements which could be able to trigger large faults if damaged. Figure 14 shows the disruption expected in the area of the city of Florence upon the production of synthetic earthquake in a nearby Apennines area.

A further CIPCast operation mode allows to insert punctual damages by hand, by the operator. Some CI element failure (belonging to one or more infrastructures) could be inserted and the Impact Scenario (with its Consequence Analysis) estimated accordingly. This operation mode (Damage Simulator) could be used to estimate the impact on services produced by types of damages which could hardly be thought as produced by specific natural events but could be rather related to intentional attacks (i.e. a patchy distribution of damages). Also in this case, CIPCast can be used to produce stress-tests, for highlighting elements whose fault could trigger an high impact on service(s). This can be particularly relevant for operators and authorities for planning appropriate actions for security enhancement of their assets.

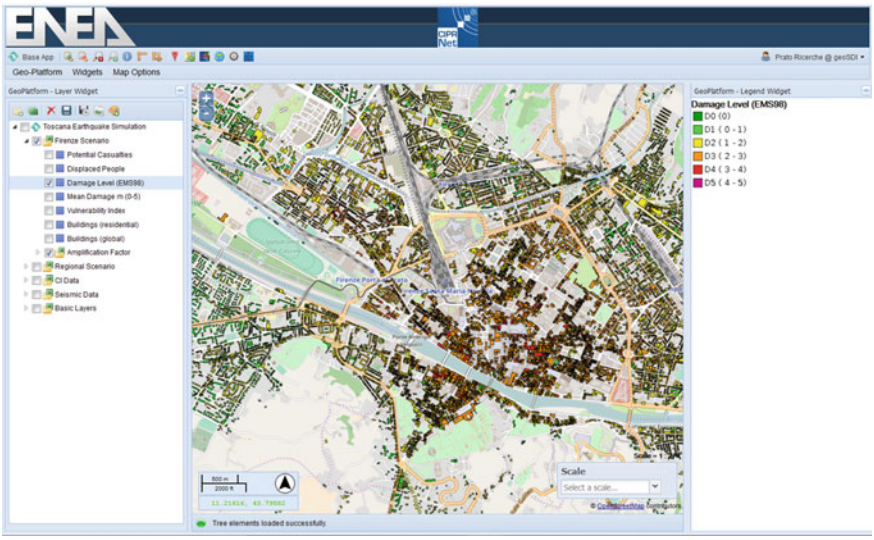


Fig. 14 Primary damages to Florence buildings induced by a strong earthquake synthetically produced in a nearby region at the north-east of the city (magnitude 6.5 Richter). Mean damages considered in a normalized 5-level scale (EMS-98)

CIPCast and its DB could act as a central system enabling to gather and to broadcast a number of relevant information, also through the use of innovative multi-media solutions. In the following we report the directions of a number of on-going project to support the usability of CIPCast contents and forecasts.

(a) CIPCast is going to integrate data on vehicle traffic status and predictions in a time span of 90 min. This information will be cast into the optimization system (RecSim) for the outage simulation in a way to drive the displacements of technical crew particularly in urban areas where traffic congestion avoidance could allow to save time and reduce the overall outage duration.
(b) Data on the paths followed by the CI networks in complex urban areas will be let available through Augmented Reality applications. These will allow a field operator (technical crews, fire fighters etc.) to have on the screen of his mobile device (smartphone, tablet) the real view of a given area (taken by the device camera) on which is superimposed the real trace of the specific network. To this trace could be associated other information (technical, contact person etc.) which might highly help the emergency or technical crews to have, on site, the largest possible information data needed to solve the problem.

11 Conclusions

CI protection and the management of Emergency situation is a major concern of Public Authorities at all scales; from the national one, as severe blackout could produce extended and often uncontrolled perturbations, to the local (city) scales where lack of resilience (i.e. lack of preparedness actions) might result in frequent, albeit limited in space and time perturbations. These, however, could produce damages on citizen's well-being, with associated economical costs, and moreover undermine citizens confidence in the public administration.

CIPCast belongs to a new class of DSS which attempts to act at three different levels:

(a) the "operational" level, by producing an operational (24/7) state of risk of CI allowing operators and Public Authorities to undertake preparedness actions;
(b) At the emergency level, CIPCast can be used as a coordination tools for sharing information at different;
(c) At the level of elaboration of contingency plan, by stress testing the CI networks.

Being usable in different operational modes (either fed with 24/7 real time data or by synthetic events of with synthetic damages), CIPCast could be a mean for stress-testing, planning, design of new generation networks and design of coherent contingency plans which could be the result of ad hoc simulations where realistic conditions could be reproduced.

Acknowledgement and Disclaimer This chapter was derived from the FP7 project CIPRNet, which has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no. 312450.

The contents of this chapter do not necessarily reflect the official opinion of the European Union. Responsibility for the information and views expressed herein lies entirely with the author(s).

Appendix 1

The availability of a large amount of data has allowed, only for the Citizens Sectors, to define, for each service and for each Sector elements, the time variation of SAW indices along the course of the day. As the priority could not be constant, the objective is therefore to condense in a graph the possible variations of the priority and, thus, the subsequent variation of the SAW indices.

In order to provide a priority index to each "service" enabled by electricity, for each Sector element and with a granularity of 30 min we set the priority value to

- 1: if the service is most likely needed. Example: lighting in the early morning or in the evening.
- 0.5: if the service may not be needed but—should it be needed—would be critical. Example: lighting late at night, when most people is sleeping.
- 0: if not needed or not a big issue if missing. Example: lighting at home whenever people is at work, or also lighting at noon.
- 0.1: for loads and services which can generally be postponed. Example: dish-washer or washing machine.

In order to perform this exercise, we have profiled the users as follows:

- Citizens 18–64: working or studying, they get up at 6 a.m., go sleeping at 11.30 p.m., leave home at 8.30 a.m. at the latest and return home at 4.30 p.m. at the earliest. Breakfast is usually between 6.00 a.m. and 7.30 a.m., dinner between 8.00 p.m. and 9.00 p.m.
- Citizens 65+: retired from work, getting up at 6 a.m. and going to bed at 11.00 p.m., they could be at home at any time. Breakfast is usually between 6.00 a.m. and 7.30 a.m., lunch between 12.30 p.m. and 1.30 p.m., dinner between 7.30 p.m. and 8.30 p.m.
- Citizens 0–5: getting up at 6.30 a.m. and going to bed at 9.30 p.m. on average, they usually are not at home between 8.30 a.m. and 4.30 p.m. if they are older than 3, while—if younger than 3—the younger the more likely that they are at home.

Using these profiles, we have determined the following global relevance index for electricity needs for the three Citizens Sector elements (age 18–64, age >65 and age <5) (Fig. 15).

Using a similar approach, we can identify the relevance of the other PS. The following graphs show the (not normalised) temporal profile of the relevance

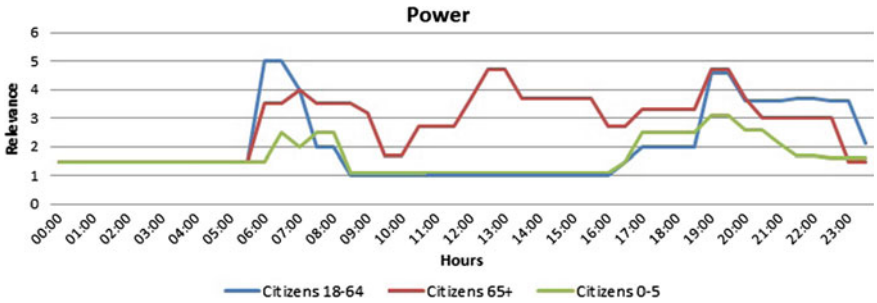


Fig. 15 Temporal profile of the relevance of electrical power for different population segments

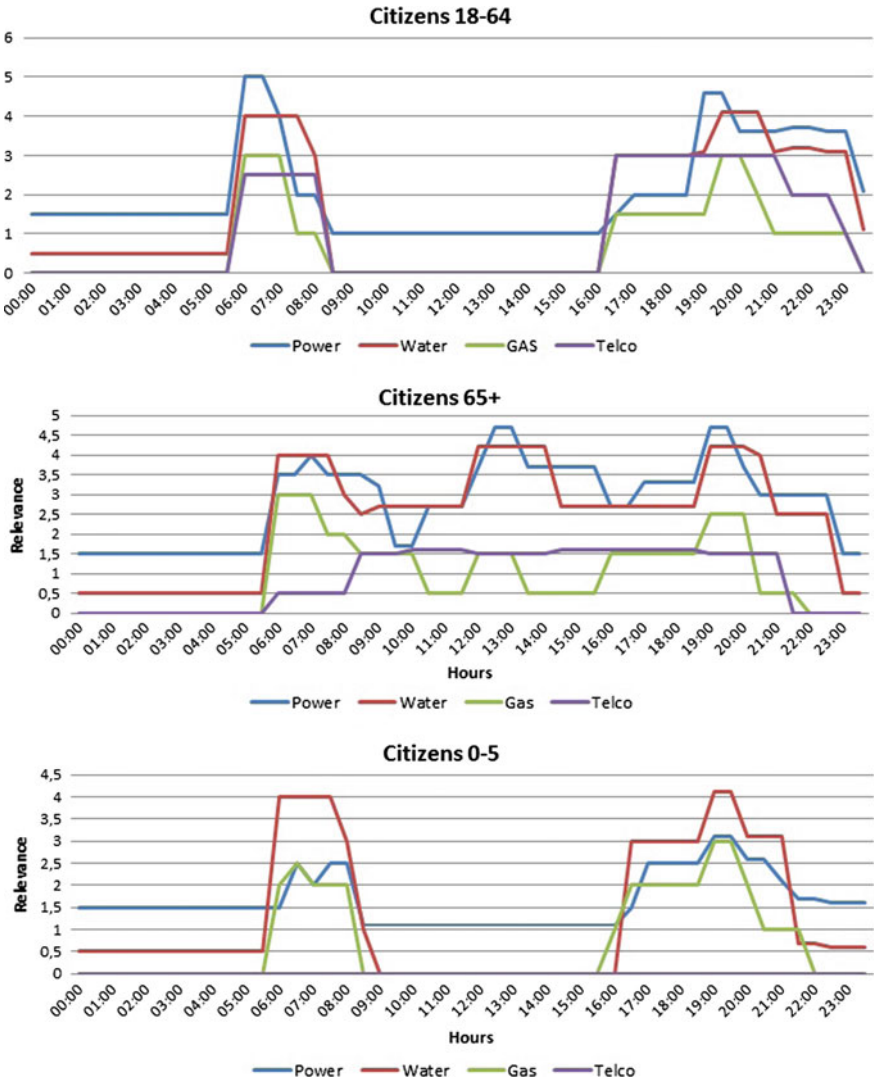


Fig. 16 Temporal profile of the relevance of CIs for the different classes of the sector "Citizens"

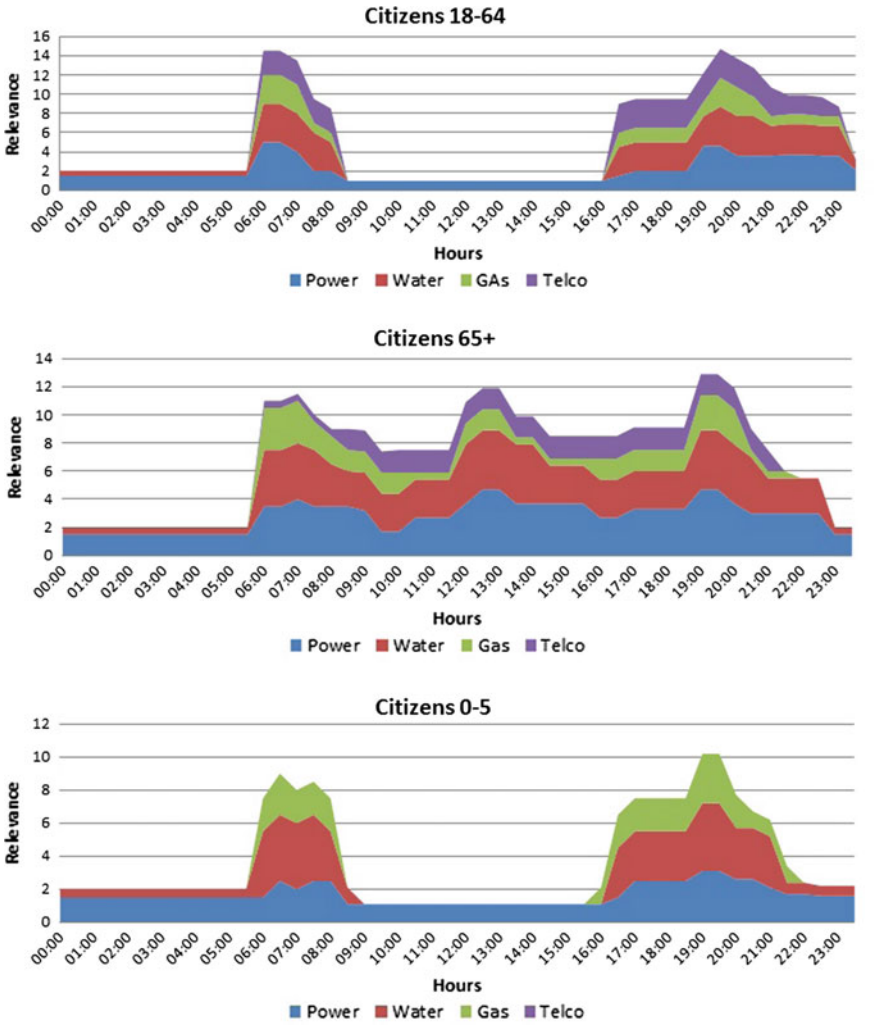


Fig. 17 Cumulative temporal profile of the relevance of CIs for the different classes of the sector "Citizens"

emphasising the absolute value (Fig. 16) and the contribute (Fig. 17) of each CI to the well-being of the citizens.

The following graphs (Fig. 18) show the relevance of each CI for different population segments.

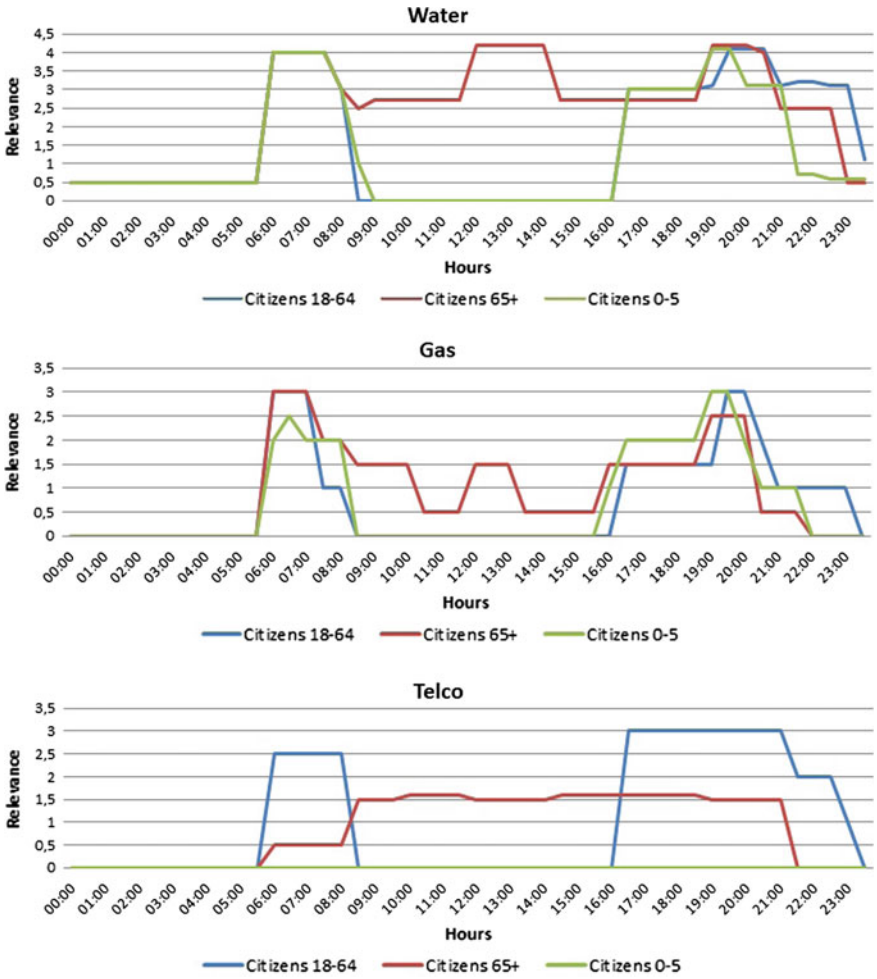


Fig. 18 The estimated temporal profile of the relevance of water, gas and telecommunication services for the different population segments

Appendix 2

The input-output matrices are $n \times n$ matrices representing the mutual relations between the various economical activities, showing, which and how, goods and services produced (output) by each activity are used as inputs by other Sector for their production processes. These data are usually released by the National Institute of Statistics and acknowledged in the national accounts of many countries.

More in details provided data are:

- a branch-by-branch table indicating the amount of production of each branch used for the production in the others;
- a product table for the product, indicating the products needed for the production of each product.

Let us consider a basic example [6].
Table 9 (read by row) indicates that

- Agriculture produces 30 quintals of wheat, 7.5 of them being consumed by itself (seeds), 6 from industry and 16.5 by the families (wheat, meat, fruit, etc.).
- Industry produces 50 m of cloth, of which: 14 m are consumed by agriculture, 6 by the industry itself and 30 by families;
- Households provide in total of 300 man-years (300 men engaged in the work the whole year), and the above table tell us also that 80 of them are employed in agriculture (farmers), 180 in industry (workers) and 40 are employed in house works.

On the other hand (reading the same table by columns):

- Agriculture employs 7.5 quintals of wheat, 14 m of cloth to 80 man-years to produce 30 quintals of wheat;
- Industry employs 6 tons of wheat, 6 m of fabric and 180 man-years to produce 50 meters of cloth;
- families spend their earned income to buy 16.5 tons of grain, 30 m of fabric and 40 years-working man to sustain life of 300 man-year.

The price system ensures the effective possibility of exchanging goods between different sectors; in the case of Table 10, prices are 20 euro for a quintal of wheat,

Table 9 Simplified model for an economy with three sectors

To	From			
	Agriculture	Industry	Households	Total
Agriculture	7.5	6	16.5	30 quintals of wheat
Industry	14	6	30	50 meters of cloth
Household	80	180	40	300 man-years of effort

Table 10 Simplified input-out value model for an economy with three sectors

To	From			
	Agriculture	Industry	Households	Total
Agriculture	150	120	330	600
Industry	210	90	450	750
Household	240	540	120	900
Total	600	750	900	2250

Table 11 Relevance of the different services for allowing production in the three main industrial sectors

CA criteria	Services				
	Electricity	Telecom	Water	Gas	Mobility
Primary t_{31}	0.4	0.06	0.186	N/A	0.408
Secondary t_{32}	0.3	0.058	0.23	N/A	0.411
Tertiary t_{33}	0.197	0.248	0.185	N/A	0.37

15 euro for a meter of cloth, 3 euro for a year-working man. This results in the following table of values.

The first line shows that the agricultural sector uses 150 euro of its product (direct use or farmer exchange), it sells part of the industry for 120 euro and the rest to families for 330 euro, with a total revenue of 600 euro.

In the same way—with the assumption that all money spent by industry contributes to the production and, thus, to the turnout—we grouped all industries (with different NACE codes) in Primary, Secondary and Tertiary sectors and then we calculated, for each sector, the fraction of the whole budget they spent for the different CI related services. We found where relevance for Gas is not available as in the input-output matrices Electricity and Gas are considered in the same PS (Table 11).

References

1. Tofani A, Di Pietro A, Lavalle L, Pollino M, Rosato V (2015) Supporting decision makers in crisis management involving interdependent critical infrastructures. The International Emergency Management Society (TIEMS), 2015
2. Di Pietro A, Wang T, Tofani A, Marti A, Pollino M, Martì JR (2015) Simulation of primary service degradations for crisis management operations. The International Emergency Management Society (TIEMS), 2015
3. http://www.eerg.it/index.php?p=Progetti_-_MICENE. Last accessed 30.06.2015
4. http://www.eerg.it/resource/pages/it/Progetti_-_MICENE/compendio_misure_consumi_elettrici.pdf. Last accessed 30.06.2015
5. De Franceschi D (2011) Analisi dei consumi energetici residenziali e vantaggi connessi all'utilizzo di un manager energetico. Master degree thesis on a measurement campaign carried out by ENEA, 2011
6. Leontief W (1986) Input-output analysis. In: Input–output economics, pp 19–40

Chapter 10
The Use of What-If Analysis to Improve the Management of Crisis Situations

Erich Rome, Thomas Doll, Stefan Rilling, Betim Sojeva, Norman Voß and Jingquan Xie

Abstract The EU FP7 Network of Excellence CIPRNet has developed CIPRTrainer, an application that provides a new capability for training crisis management (CM) staff. It enables exploring different courses of action and comparing their consequences (what-if analysis) in complex simulated crisis and emergency scenarios. The simulation employs threat, impact, and damage models and is based on federated modelling, simulation and analysis of Critical Infrastructures. In this chapter, we present an overview of the technical realisation of CIPRTrainer, embed the approach into the state of the art, and elaborate on CIPRTrainer's user interface and the training experience. The chapter also explains how the models for the complex crisis scenarios have been created, what level of detail could be realised, and how cases of missing data could be handled. As an example, we use a cross-border scenario about a cargo train derailment disaster. In the final sections, the reader learns how to set up, start and perform a training session with CIPRTrainer, how to use 'what if' analysis, and how to read the results of consequence analysis.

E. Rome (✉) · T. Doll · S. Rilling · B. Sojeva · N. Voß · J. Xie
Fraunhofer IAIS, Sankt Augustin, Germany
e-mail: erich.rome@iais.fraunhofer.de

T. Doll
e-mail: thomas.doll@iais.fraunhofer.de

S. Rilling
e-mail: stefan.rilling@iais.fraunhofer.de

B. Sojeva
e-mail: betim.sojeva@iais.fraunhofer.de

N. Voß
e-mail: norman.voss@iais.fraunhofer.de

J. Xie
e-mail: jingquan.xie@iais.fraunhofer.de

R. Setola et al. (eds.), *Managing the Complexity of Critical Infrastructures*,
Studies in Systems, Decision and Control 90,
DOI 10.1007/978-3-319-51043-9_10

List of Abbreviations

API	Application programmer interface
CA	Consequence analysis
CAM	Consequence analysis module
CEP	Complex event processing
CGE	Calculable general equilibrium
CI	Critical infrastructure
CM	Crisis management
DB	Deutsche Bahn (German railway operator)
DBMS	Database management systems
DE	Two-letter country code for Germany
ECI	European critical infrastructure
ENTSO-E	European network of transmission system operators energy
ESDB	European scenario database
fMS&A	Federated modelling, simulation and analysis
GDP	Gross domestic product
GUI	Graphical user interface
HTTP	Hypertext transfer protocol
ICE	InterCity express (German high-speed train)
IOM	Input-output model
NL	Two-letter country code for The Netherlands
NRW	North-Rhine Westphalia (federal state in Germany)
OLAP	Online analytical processing
OSM	OpenStreetMap
REST	Representational state transfer
ROOP	Resource oriented operation planning
SDL	Scenario description language
WIA	What-if analysis

1 Introduction—Role of Critical Infrastructures in Civil Crisis and Disaster Situations

The management of a disaster or crisis typically consists of cycles of situation update, analysis of the situation, decision taking, and planning and execution of response actions, sometimes under severe time pressure. At decision points, crisis managers often do not have just one option for action, but several. The challenge is to take a well-informed and most effective decision. Insufficient awareness of the role of Critical Infrastructures (CI) [1] and incomplete information on consequences of crisis or disaster evolution [2] contribute to that challenge. CI can play three main roles in crises or disasters. (1) The CI may be *affected* by a disaster. For instance, an extended flooding would most likely disable elements of the electricity, telecommunication, and sewer system infrastructures (and maybe more), with cascading effects on other

CI [3]. (2) An emergency or disaster may *emerge* from a CI. A technical failure in the electricity infrastructure may lead to a blackout and further cascading effects [4]. (3) An infrastructure may be a *resource* for response and mitigation actions. This might not be immediately obvious, but may come as a late insight when this infrastructure fails or even gets destroyed [5]. An example is a bridge in eastern Germany that was washed away by a fluvial flood. The local responders were no longer able to send forces to the other riverside, and did not have an alternative plan for that situation.

In most cases, it is not possible for crisis managers to revert a decision or an action already taken—in reality. However, in *simulation* it is possible to do exactly this: 'go back in time' and explore a different course of action. This allows answering hypothetical questions like 'What would happen if I take a different decision or follow a different course of action?'. Therefore, this is also sometimes called 'what-if analysis'. Since this type of what-if analysis requires simulation, it is rather suited for training purposes. Providing such what-if analysis as a capability to end-users is the essential idea behind the training system CIPRTrainer, which we will present in detail in the main part of this chapter.

CIPRTrainer is the software system that enables crisis managers to train decision-making in crises and emergencies involving cascading effects of CIs. CIPRTrainer constitutes an unprecedented training opportunity that complements standard command post, table-top, or physical exercises. The expected benefits would be increased awareness of crisis managers of the role and behaviour of interconnected CIs in disasters, emergencies, and crisis situations, and a better understanding of possible consequences of scenario evolution and the influence of own actions.

The remainder of this chapter is structured as follows. We continue with briefly embedding the CIPRTrainer approach to what-if analysis into the state of the art and then proceed with characterising the types of complex crisis scenarios that we designed for the CIPRTrainer prototype. Then we will give an overview of the building blocks of CIPRTrainer, explaining how we technically realised it. The following section will then provide an overview of how we realised impact and consequence analysis (CA) for the global assessment of damages and how it is employed for what-if analysis. We continue with explaining how CIPRTrainer is actually used and with an example of a training session. An outlook on the next version of CIPRTrainer and a conclusion end this chapter. For reference, we included a list of acronyms and a bibliography.

2 State of the Art: Critical Review of Literature on What-If Analysis and Federated Modelling and Simulation

What-if analysis, as a method for hypothetic data analysis, has been extensively investigated in the area of predictive business intelligence [6, 7], data warehouse [8], and in-database modelling and simulation [9, 10]. A what-if model is proposed

in [10]. It is argued in this work that the data is dead without using the what-if models to analyse them and discover insightful information from the data. Finally it drew the conclusion by pointing out that modern DBMS has certain degree of analytic support, however deep predictive analytics beyond the commonly used statistical methods are still missing. In the area of data warehouses, methodologies for what-if analysis have been proposed [8]. This methodology provides a systematic approach to design systems with what-if analysis support. A case study has also been provided to illustrate the practicality of the methodology. A dedicated online analytical processing (OLAP) query types—what-if query—was proposed in [7]. It aims to bring what-if functionalities into OLAP applications by providing a high-level syntactic structure to ease query construction. Tailored index structures have also been proposed to accelerate the query processing.

Methodologies with stochastic analysis supporting certain degrees of what-if analysis are provided in SimSQL [11]. SimSQL however focuses on the analysis of data with possible worlds in a stochastic way, which differentiates the application use cases for simulation-based decision support—as described in our approach. Nevertheless some ideas like using the possible worlds to represent and perform the simulation to gain and compare different insights of certain actions are similar. Probabilistic databases [12] provide a set of methods to handle imprecise and uncertain data with the concept of possible worlds. These systems provide built-in support for hypothetical queries, a.k.a. what-if queries to retrieve the data from different possible worlds. One example is the MayBMS [13], which is a state-of-the-art probabilistic database management system for scalable what-if queries. These works are more focusing on the efficiency of query processing in the database systems based on the probability of tuples stored in the database tables.

For modelling and simulating interconnected systems of heterogeneous CI, there are basically two approaches, namely *integrated* and *federated* simulation. In the integrated approach to modelling and simulating CI, the elements of the interconnected different CI are modelled using a single representation scheme. There is only one simulator that simulates the entire modelled CI system-of-systems. This approach is rather suited for models with a high degree of abstraction, that is, less model detail, in order to be efficiently manageable. On the positive side, the modelling and simulation is in one hand, but the designers of the models should consult domain experts for ensuring technically valid models.

An alternative approach is *federated modelling and simulation*. Here, for each considered CI a specialised domain simulator is employed. Several such simulators are then interconnected by means of some type of communication software (middleware). The whole setup is then called a federated simulation, and the component simulators are called federates. This second approach is the one that we have chosen for CIPRTrainer. An advantage is that the domain simulators are specialised on their domain and provide a correct simulation. Sometimes, it is even possible to acquire a ready-made model and just read it in as a data file in a simulator. Another advantage is that such specialised CI simulators allow for a fair level of detail and thus provide better scalability than integrated simulations. A drawback is that

typically all the models or data formats of the federates are different and require familiarisation and domain expertise.

Practically all federated CI simulations are results of research projects. Some of them have been used and are being further developed in agencies or national or EU labs. Rome et al. [14] have provided an elaborate state of the art chapter on federated modelling and simulation. They write:

> The characterised works […] can be divided roughly into three—not entirely disjunct—categories:
>
> 1. Special purpose federated simulation systems, consisting of a number of simulators (CI and others), additional system components, and a dedicated middleware for communication and synchronisation (IRRIIS, EPOCHS, …),
> 2. Frameworks for modelling, simulation and analysis of CI using dedicated—for instance, agent-based—simulations (I2Sim, AIMS, IME, …),
> 3. More general frameworks for setting up distributed federations and more general middleware for communication and synchronisation within federations (IDSim, ASimJava, …), including (quasi-)standards (OpenMI, HLA, …), and sometimes accompanied by proofs-of-concept (DIESIS, XMSF, WSIM, …).

We would recommend the reader to resort to [14] for an in-depth review of state-of-the-art federated modelling and simulation frameworks and systems.

3 What-If Analysis—A New Capability for Training Crisis Management Staff

The what-if analysis capability of CIPRTrainer enables trainees to explore different courses of Crisis Management (CM) actions in a computer-based simulation (Fig. 1). CIPRTrainer displays information on events that happen in the simulation, like a derailment of a cargo train. The system has an inventory of actions available

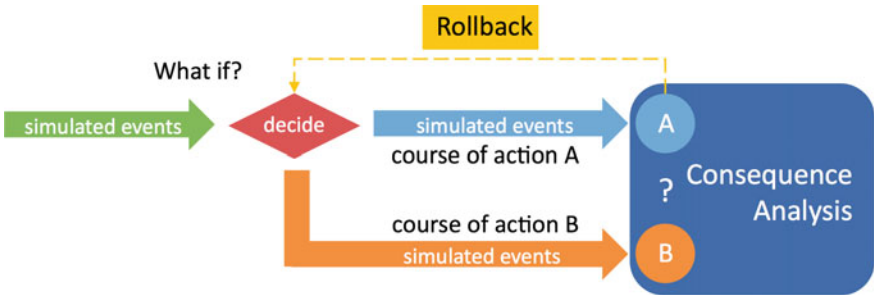


Fig. 1 What-if analysis: after taking course of action *A*, the trainee may perform a rollback to a decision point, and take a different course of action *B*. The trainee can use consequence analysis to compare the overall consequences of both scenario evolutions

for reacting on the occurring events. Rules within CIPRTrainer provide some additional flexibility. For instance, if a certain response action is being performed by the trainee within a given time window, then it would prevent some disastrous event from happening.

At any time after the simulation started, the trainee may choose to 'go back in time'—or, as we call it, perform a *rollback*—and explore a different course of action. In order to do this, the trainee must select one of the previously performed actions, and then perform the rollback. CIPRTrainer then resets the simulation into the state that it had before the selected past action. By following a different course of action, the trainee creates another version of the simulated 'world'.

Such rollbacks can be performed multiple times. Since the history of all performed actions is recorded, the generated courses of actions form a tree-like structure. CIPRTrainer can display this structure for providing an overview of the training activities.

A core element of the training is evaluating the training session and the performed courses of action. The trainee shall be enabled to find out how the chosen courses of action influenced the overall outcome or consequences of the simulated crisis or disaster. For doing this, the tree-like visual representation of the courses of action serves as starting point for performing CA.

CIPRTrainer contains a Consequence Analysis Module (CAM), which enables the user to understand the consequences (in terms of harm to humans, degradation of CI services and monetary losses) of the simulated impacts and of the chosen actions (or inactions). The CAM utilises data from the CIPRTrainer database, and an array of methods implemented for calculating the consequences for the population, and the critical and non-CI in the affected region.

4 Scenarios for Training

One design goal of CIPRTrainer was a wide applicability of the system, including crisis situations with cross-border effects. We picked a region spanning both sides of the border of two countries represented in the CIPRNet consortium: Germany and The Netherlands. The geographical location is restricted to the Kleve district in Germany and the city region of Arnhem-Nijmegen in the Netherlands. The area is prone to flooding by high water levels of the river Rhine. Also, it contains a number of infrastructures, like the railway line connecting Rotterdam harbour with the European hinterland. In this setting we designed two storylines in a complex scenario with cross-border effects [15]. One is the derailment of a cargo train in the German city of Emmerich, and the second one is an extended flooding of the area by the river Rhine.

For the development of the scenarios, we started with research on information and data from the considered regions. Data are the basis for modelling the scenario on the computer. Some of the modelled CI networks are fictive for two reasons:

first, we did not have data on some of these networks and second, for security reasons, since we did not want to disclose sensitive information. We employed the domain expertise of the consortium, including electrical and telecommunications engineers, security professionals, and experts in railway security, cyber security, crisis management, and the water domain. External expertise was provided by the head of the fire-fighters in a large German city, and experts from CIPRNet's international advisory board. Later in this chapter, we will describe in more detail two specific aspects of modelling: (1) the modelling of networks of interconnected CI and (2) modelling for CA. More technical details of the modelling activities can be found in CIPRNet deliverables D6.2 [16], D6.3 [17] and D6.4 [18].

5 CIPRTrainer

The CIPRTrainer system consists of *software* and *data*. The software part, the application or computer programme called 'CIPRTrainer', can be considered the machinery that performs the simulation. The data part, stored in CIPRTrainer's database, consists of the computer models of the crisis or disaster scenarios, that is, artificial 'worlds' based on data and information of real geographical locations and hypothetical dangerous incidents. Understanding the new what-if analysis capability requires a basic understanding of scope and limitations of both parts. Therefore, this section will address both the scenario models and the CIPRTrainer system.

5.1 System Description

CIPRTrainer is a software system that provides training services to crisis managers for decision-making in crisis situations. Its strength is the ability to simulate complex crisis scenarios including cascading effects of CI disruptions. It is designed with flexibility in mind. Federated simulation is adopted to enhance the training by providing realistic system dynamics. Geo-spatial information is integrated seamlessly into this system to enhance the location-aware situational awareness. Complex Event Processing (CEP) provides a declarative means to glue the dynamics of different components. Finally, all of the system components are technically integrated with the lightweight RESTful Web Services. From the functional perspective, CIPRTrainer consists of two major building blocks, a **design engine** and a **training engine**, which will be elaborated in the following sub-sections. An overview of all the building blocks and the data flow between them is depicted in Fig. 2.

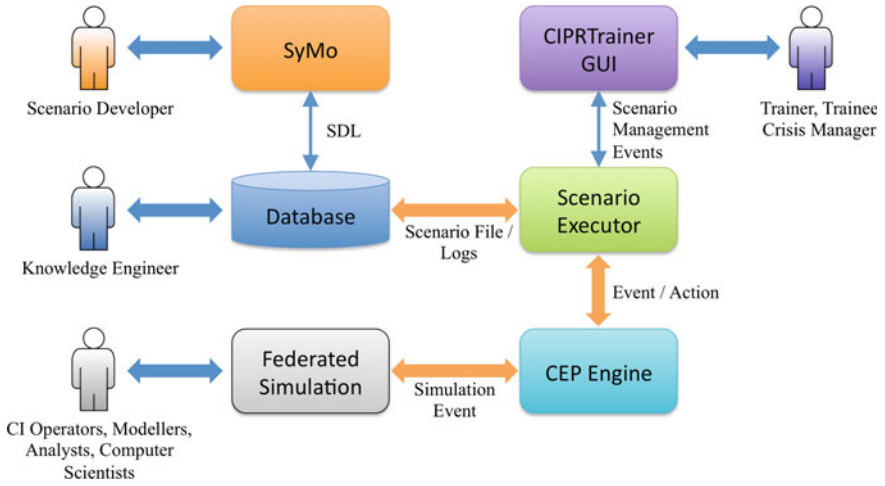


Fig. 2 Building blocks of CIPRTrainer. The CIPRTrainer graphical user interface is the part with which trainer and trainees interact. 'SyMo' refers to the scenario editor, the toll with which the static modelling activities are started. The other four components constitute CIPRTrainer's 'backend', that is, the internal simulation machinery. The heterogeneous modelling activities for setting up a scenario precede the regular usage for training. A knowledge engineer adds model parts to the database, and domain experts provide CI models to the federated CI simulation

5.1.1 Design Engine

For the CIPRNet project SyMo (System Modeller) is used as a scenario editor. SyMo is a tool developed by Fraunhofer since 2008 and it is used in various projects for modelling and analysis purposes. The main advantage in using SyMo for the creation of the scenarios is that all necessary elements, tools for concatenation, sequence control, syntax checks and even semantic examination are already implemented and incorporated inside a graphical user interface. Scenario models in SyMo are two-part and consist of a static model and the dependencies between elements of the static model. Typically, the tree-like static model (Fig. 3) may contain components like an organisational structure, a taxonomy, technical systems, events, resources etc. The model representation generated with SyMo contains some variables and parameters, which allow creating different storylines within the scenario.

Modelling with SyMo consists of three steps:

1. Create a static model and a process model of the scenario
2. Configure the model by choosing concrete values for variables and parameters
3. Export the configured SyMo model into a scenario file and store it in the CIPRTrainer scenario database.

The modelling of the scenario storylines for CIPRNet follows an approach that is called resource oriented operation planning (ROOP). The basic idea is that

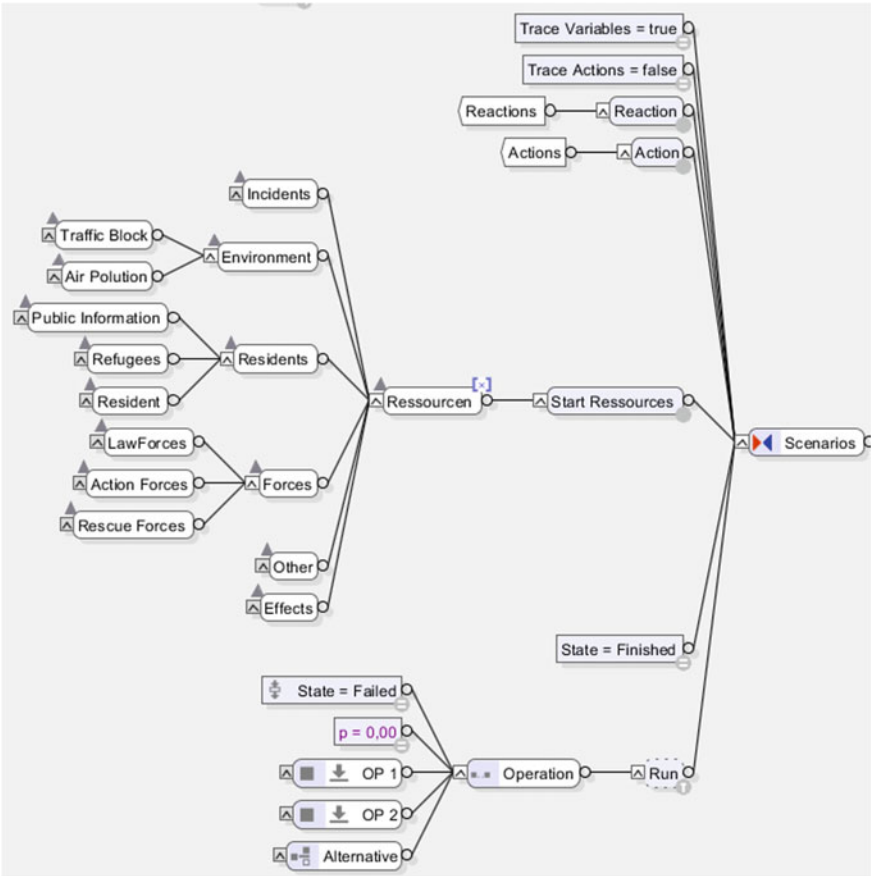


Fig. 3 Snapshot of a scenario model created with the Scenario Editor based on SyMo

counteracting a disaster is a matter of available resources, remaining time, and situation of the disaster (like location and effects/impacts of incidents). The available resources at any given point in time limit the possibilities of response and mitigation actions. The situation of the disaster determines what would need to be done to counteract (or fight) it. Thus it is important to keep track of the used resources and the evolution of the disaster. Responders and action forces are considered and modelled as resources. In a uniform way, the attributes of the situation of the disaster are also modelled as "resources". This is a legacy from using SyMo in the military context. The disaster could be considered a "foe" and the responders as "friend". Both have resources and "use" them to "fight" each other.

For modelling the disaster incidents and the disaster management and response actions in the affected area, it is important to also know the locations of the resources. In order to facilitate the modelling in this respect, we start with partitioning the area where the disaster happens into zones. Using zones allows a simpler and quicker

processing of geographical interactions. The zone borders are manually defined and oriented along landmarks such as rivers, main streets, railway tracks, historic city centres etc. Having done this, we just need to know in which zone which action shall be applied or response forces are located and their strengths. We do not need to know the exact positions of, for instance, each fire-fighter at any given point in time. The Emmerich scenario area is arbitrarily divided into 15 zones.

The top-level model of the "scenario components" consists of resources, locations, effects and two technical elements, namely measurement units and a resource generator. The top-level model of the "incident related aspects" consists of reactions, actions, action patterns, parameters and a technical component named "scenarios". After defining the involved scenario components as attributes and variables, the interaction of the components is modelled. Different operators are applied to model the incidents, reactions and actions performed in a given time span. There are seven operators for different tasks:

- Sequence
- Parallel
- Race
- Action
- Alternative
- Iterator
- Call

The sequence operator executes the subsequent tasks sequentially. The parallel operator performs the tasks all at once. The race operator will execute the tasks in parallel and only evaluate the task that is finished first. The action operator simply executes the given task. The alternative operator leaves a second choice for the case that the first task cannot be successfully performed. The iterator operator is used for defining tasks that are then executed repeatedly in a loop. The call operator behaves like the action operator. The only difference is that a sub function is called in contrast to executing an action directly. With these operators it is possible to model the incident related aspects of the scenario. For instance, the actions are modelled as a sequence of operations with alternatives for deploying the forces and parallel operations for moving the different forces from different locations.

After modelling the scenario details within SyMo and configuring and creating the scenario file, the resulting file can be parsed and serialised into a flat file conforming the Scenario Description Language (SDL) [15]. The event-processing engine for initialisation of the start resources can then read the different operators, variables and timestamps and in addition events and actions are read and written into the event queue. The events and actions are ordered using the given timestamps from the SyMo model. Execution of all events and actions with timestamp = 1 can then be executed by starting the event processor. The given events are then processed using special rules. These rules decide which events should be forwarded to the simulators and what actions the simulators have to perform as reaction.

5.1.2 Training Engine

The training engine of CIPRTrainer is a modern web-based application, which accepts the scenario description files from the design engine. It basically contains two parts: the front-end GUI and the backend machinery.

The front-end GUI is a standard web application, which uses modern web technologies [19]. It is accessible through the regular HTTP/HTTPS protocol. The front-end is implemented using a variant of the classic MVC (Model-View-Controller) framework; see the right part of Fig. 4. The content is loaded dynamically by sending asynchronous requests and receiving push notifications from the application server.[1] The system embraces a three-tier-architecture, which contains a presentation, logic and data-tier (see Fig. 4 the left). The front-end (presentation-tier) is implemented using the AngularJS framework. It provides models that are bound to the view-layer. These models can be manipulated through its controller-functions. Its service-functions handle typically the communication to the services. The web or application-server (logic-tier) incorporates an event-driven runtime environment. It incorporates the application- and business logic, and provides a RESTful Web Services for what-if analysis and other capabilities. The application server also includes scenario services, and the federated simulation controller that is able to set up, start and stop the federated simulation. The web-server has access to the databases, which serialize spatial- and socio-demographic data, CI models, user configurations and training protocols. In general, the front-end GUI contains the following functional blocks:

- **System authentication**. Each training session starts with an authentication. Using the application require user authentication: users have to launch the application by opening the browser and entering the domain name on which the CIPRTrainer web-server is listening. The landing page offers a navigation-bar on which the user is able to log into the system entering username and password. Based on the user role, he or she may enter the training mode or the trainer dashboard.
- **Trainee view**. CIs or resources are represented as GIS markers containing CI- or resource-specific icons. Icons are carefully chosen in order to avoid misinterpretations. Crisis managers use specific tactical symbols that represent events and current states on the map. Moreover, for a crisis manager it is important to immediately know the operational status of CIs.
- **Trainer dashboard**. The trainer is able to log into the dashboard that monitors the evolution of the running training session including information about the trainee, the trainee's actions, scenario state, and CA results. The user also has the possibility to choose, start and stop scenario, and assign a participant to a training session. Moreover, the computed CA and training protocols are downloadable in CSV or JSON format.

[1] https://nodejs.org.

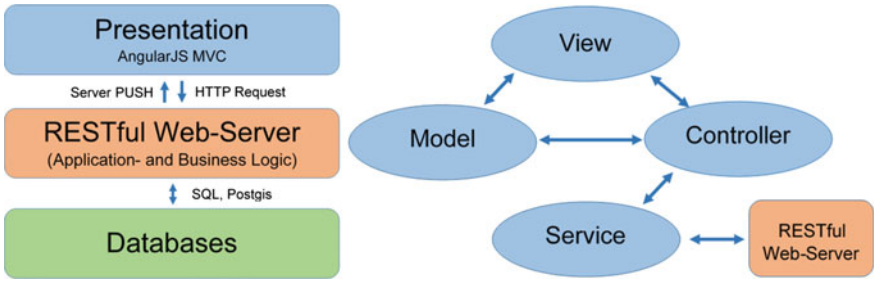


Fig. 4 System architecture of the CIPRTrainer (*left*) and AngularJS MVC pattern (*right*)

- **Timeline**. The timeline displays a set of different events in a chronological order. These events can be pre-defined scenario events (accident, explosion, etc.) or events that are calculated by the federated simulators. Also, it can display different kind of actions, which can be performed by the crisis manager. Lastly, external sources of information are displayed on the timeline, which can origin from other agencies such as police or fire-fighters. A crucial advantage of displaying a chronological set of events is that the crisis manager can keep track of all kind of information sources. The user is able to focus on specific time intervals and thereby focus on important events and hide less important ones by dragging and zooming onto the timeline. Therefore, the user is able to comprehend the complete scenario and thus make better decisions.
- **Internationalisation support**. The CIPRTrainer supports various languages (currently Dutch, German, and English). The user can choose a desired language by clicking on the listed flag on the navigation bar. The CIPRTrainer is able to depict tactical symbols of resources like police, fire-fighters or hospitals based on the end-user's localisation. Crisis managers from the Netherlands utilise different tactical symbols than German crisis managers. The CIPRTrainer includes a set of tactical symbols for each country. Currently, German and Dutch tactical symbols are incorporated into the CIPRTrainer.
- **Action execution**. Actions influence the state of the critical infrastructure and the result of the consequence analysis. The trainee has two types of actions: (1) First responder actions; (2) Crisis management actions. The first type of action involves actual forces/resources, which are spread in the region of Emmerich. The capacities are presented as triple (leader, sub-leader and forces). The accumulation of these three values refers to the capacity strength of a specific unit. The user is able to send resources with a certain capacity to the crisis region. The second type of actions is suited for crisis managers. A crisis manager is able to alarm public authorities and the general public as well as evacuate critical regions. Each action influences the consequences in the scenario.
- **Action tree**. The CIPRTrainer allows the end-user to select and compare consequences of different courses of action. Performed actions and their

chronological order are visualized as a multidimensional tree. Each node represents a performed action. Whenever the user jumps back to a prior action x_t (perform a rollback), the CIPRTrainer automatically creates a new branch on action x_t, on which upcoming actions will be added. The result is a multidimensional tree that reflects the trainee's decisions throughout the entire training session. The leaves of the n-dimensional tree are the last performed actions of which each the user is able to acquire the consequence analysis of the entire action chain back to the initial state node of the tree.

The backend of CIPRTrainer contains basically two parts: (1) the **business logic layer** that reside in the application servers and the rule base of the CEP engine; (2) the **persistence layer** where all relevant data is stored and managed in a single instance of PostgreSQL database.

The business logic of CIPRTrainer backend is mainly developed as a NodeJS application. User sends requests to the web server, which then redirects the request to a private IP address on which the application server listens. Typically, a web application consists of various configuration files (server and database configuration, etc.), a front-end implementation, set of views and routes, and a logic tier. The main configuration of the server incorporates an HTTP web-server definitions and references to the RESTful endpoints. Any other sort of configurations that do not deal with the application logics, such as database connections and web mapping configurations, are separated in other configurations. The server implementation including route end-points, views, and server specific services are located in the server folder.

Scenarios allow crisis managers to outline a sequence of events and provide the basis for the performing the CA, thus evaluating susceptibilities of CIs by revealing dependencies, interdependencies and cascading effects (see [20–22]). Part of the scenario is the storyline, a set of events that could happen during the scenario running. Scenario executor controls the heartbeat of the whole system. It maps the simulation time and real wall time. For instance, to accelerate the simulation, the scale can be 60:1, i.e. 60 simulation seconds should be done within one real time second. Under this setting, two situations can happen:

- The system is fast enough and the actual execution time is less than one real time second. Therefore some kind of `sleep` mechanisms will be introduced before the simulation for the next 60 simulation seconds is started.
- The system is not fast enough to finish the simulation within the given time frame. That means, it is not possible to simulate 60 s within one real time second. The scaling factor will be modified based on the best system performance, e.g. 10:1—just simulate 10 simulation seconds instead of 60.

The trainer can initialise (load the storyline of the scenario) and start or stop the scenario executor. Each event in the storyline is annotated with a timestamp t_i. Once the simulation time t_s passes t_i, the scenario executor notifies CEP-Engine and the CIPRTrainer by sending a HTTP push-request containing event-specific data (see Fig. 5). This way, the trainee can see events on the map including GPS coordinates,

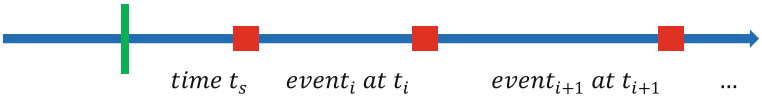


Fig. 5 Once the simulation time t_s passes t_i, CEP-engine and CIPRTrainer will be notified by sending a HTTP push-request containing event-specific data

event-specific information and a tactical symbol describing the event. The trainee can pause and continue the training.

In addition to the scenario executor, the **mapping service** is also one of the core stones in the business layer. The WMS standard is used for acquiring rasterised spatial data such as base layer maps. Another important standard is the Web Feature Service Interface Standard that provides an interface specification for requesting spatial features. It provides vectorised data in various formats such as shapefiles and GeoJSON, etc. MapServer is an open source platform of providing spatial features for GIS applications that incorporates both OGC standards WMS and WFS (see Fig. 6). CIPRTrainer uses it to receive vectorised features like the CI models of the simulators and resources (police, fire-fighters, hospitals, etc.). We use the WMS standard to show flooding on the base layer.

In order to expose the simulation model to the CIPRTrainer, a facade database is developed that aggregates all the involved CI models. The WFS/WMS services extract the relevant information at runtime and push it to the CIPRTrainer front-end. The information includes:

- Geospatial information of CI elements like the coordination of a transformer, the polygon of a railway main station or the polyline of a railway track.

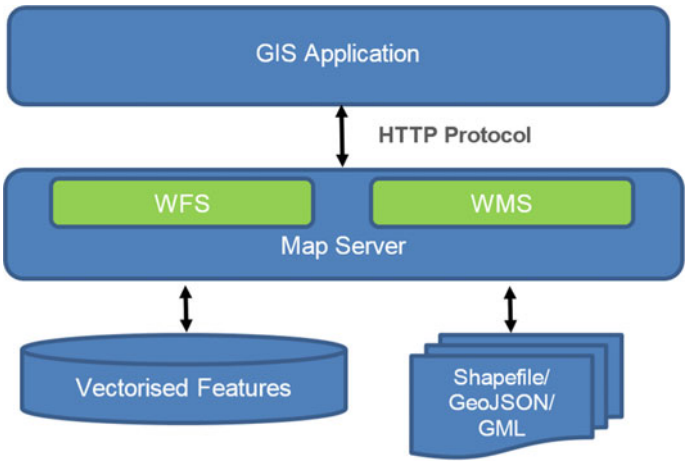


Fig. 6 MapServer implements the OGC Standards WFS and WMS that provide rasterised and vectorised spatial data for rich GIS applications. Spatial data can be stored in relational databases (e.g. PostgreSQL + PostGIS extension) or files that can have various formats (GeoJSON, ESRI Shapefile)

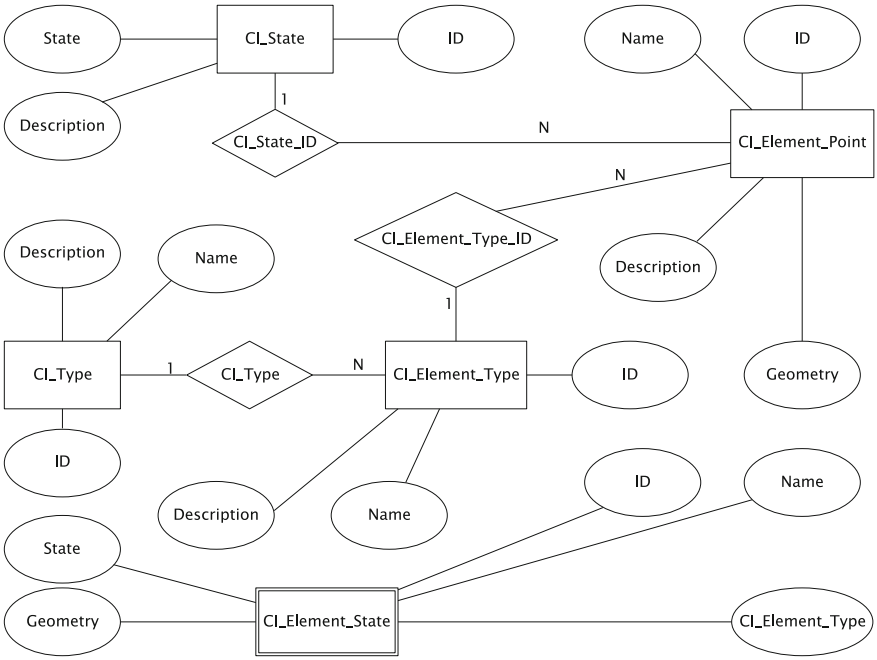


Fig. 7 Entity-relationship (ER) diagram of the CI element state database

- The state information of CI elements like **normal**, **stressed**, **failed** and **recovery**.
- Meta-information like the name, a short description of the CI.

The database design is illustrated in Fig. 7 as an Entity-Relationship diagram in Chen syntax. The design follows strictly the database normalisation form to remove redundancy information storage. Redundant information is provided as various database views (without physically materialise it to the physical storage like hard disks) to ease the access from outside. In general there are several entities listed below:

1. The entity `CI_State` denotes the possible states of a CI or CI element. Basically in the implemented database table, the `State` column contains the four states defined in, i.e. `normal`, `stressed`, `failed` and `recovery`.
2. The entity `CI_Type` contains the domains of CI like electrical network, telecommunication network and railway network.
3. The entity `CI_Element_Type` is about concrete CI elements like a transformer in the electrical network or a router in a telecommunication network. It is different than the `CI_Type` entity. A `CI_Type` can contain multiple types of `CI_Element_Type`. For instance, if the CI is an electrical network, then its element types are transformers, sub-stations, power poles, etc.
4. The entity `CI_Element_Point` models the real instance of the CI elements. It includes the name of the CI element, a short description, the element types and

most importantly the state information and the geo-location. The current design of the database distinguishes CI elements with geometry type `POINT`, `POLYLINE` and `POLYGON`. The reason for this kind of different handling lies in the efficient modelling capability provided by PostGIS, which is used in the database system to handle geospatial objects. In order to efficiently query and store different kinds of spatial objects, the types must be provided during the schema generation phase. In Fig. 7, only the CI element with geometry type POINT is illustrated.

5.2 Federated Modelling and Simulation

For achieving a plausible simulation of the behaviour of CI under perturbations, including failures and cascading effects that propagate failures to other dependent CI, CIPRTrainer employs two commercial simulators (SIEMENS PSS© SINCAL for electricity networks and OpenTrack for railway networks) and one free simulator (ns-3 for telecommunication networks). All these simulators are supplied with models of CI in the scenario area, which are either real or realistic artificial CI models. Information on dependencies between interconnected infrastructures, like which electricity CI element supplies which telecommunication CI element with power, are stored in a database. A failure of the former element triggers a stressed state or failure of the latter element.

Such state changes are represented by software 'events' in CIPRTrainer. Each of the simulators is connected to the rest of the CIPRTrainer system by a special 'connector' that translates 'events' into a format that the simulator can understand. Such a setup of connected stand-alone simulators is called a *federated simulation*. The 'connectors' are also employed for synchronising the simulators and for enabling the rollback.

5.2.1 Building CI Simulation Models

The federated simulation environment consists of CI models, dedicated domain specific simulators including both CI simulators and threat simulators, and the simulator connectors that enable the communication with other CIPRTrainer components. In its current state, the CIPRTrainer system's simulation component is able to simulate electricity, telecommunication and railway infrastructure through the interconnection of dedicated simulators for these types of infrastructures.

For each simulator, a simulation model that reflects the real-world conditions needs to be set up. This process can be compared to the content creation step of traditional video games and involves, due to the needed expert knowledge, a significant part of manual work. To build up a realistic or at least plausible simulation model that matches the real-world infrastructure, data sources like maps or construction plans need to be taken into account. During the modelling process, it

turned out that a part of the information needed is available to the public and on an appropriate level of detail. However, the publication of data revealing the details of CIs might raise security issues, therefore, a significant amount of data is not available to a public audience. For example, the details of electrical distribution networks are not traceable through the Internet.

For the implementation of the cross-border derailment and flooding scenario in the Emmerich area, we used the simulators PSS®SINCAL [23] for the modelling and simulation of the electrical transmission and distribution network, the Network Simulation version 3 tools (ns-3) to model and simulate the telecommunication network [24], and the railway simulation software OpenTrack [25] to model and simulate the railway infrastructure.

The model of the electrical transmission network around Emmerich was created manually based on the available data using the graphical user interface of the PSS®SINCAL software. The data adopted to build up the model is partially based on OpenStreetMap (OSM) and most of this data seemed to be valid (we checked this for instance, by comparing the geo location with other Google satellite images). The ENTSO-E database can furthermore serve as a means for verification. However, as volunteers collect OpenStreetMap data, there is always no guarantee that OSM data always match the real world. The model of the electrical distribution network within the area of the city of Emmerich is purely fictive, due to the lack of available data sources. The model was built by experts in the field and took a typical city with the size of Emmerich as foundation. An overview of the distribution network model can be seen within Fig. 8.

The structure of this model is based on a typical distribution network of a small city, the constraints and particularities given by the transmission network and the topographic structure of the city were taken into account. The distribution network is modelled up to the 20 kV medium voltage distribution network layer, with cabinet feeders as the endpoints of the network. Each of the cabinet feeders transforms the 20 kV electrical voltages to 400 V low voltages that are delivered to the single houses. As the model does not cover the low voltage network, each cabinet feeder provides power supply to a specific small area within the city and therefore usually supplies several houses with power. In dedicated zones, i.e. industrial areas or the Emmerich harbour area, the model comprises single cabinet feeders, which provide higher output voltages.

The process of creating an imaginary, but plausible CI model was also carried through for the creation of the telecommunication infrastructure model, as in this case, similar to the electrical distribution network, no useful data was available to the public. The model consists of routers, cell towers and interconnecting telecommunication lines. Figure 9 shows an overview of the telecommunication network within the city of Emmerich. The model was also set up by experts in the field, for the positioning of the according routers; the infrastructure of the city was taken into account. For example, several routers were placed close to police stations, schools or hospitals or close to power substations to simulate the need of optimal access to the telecommunication network by these facilities. The course of the telecommunication cables was also adjusted to the need of the CIPRTrainer's

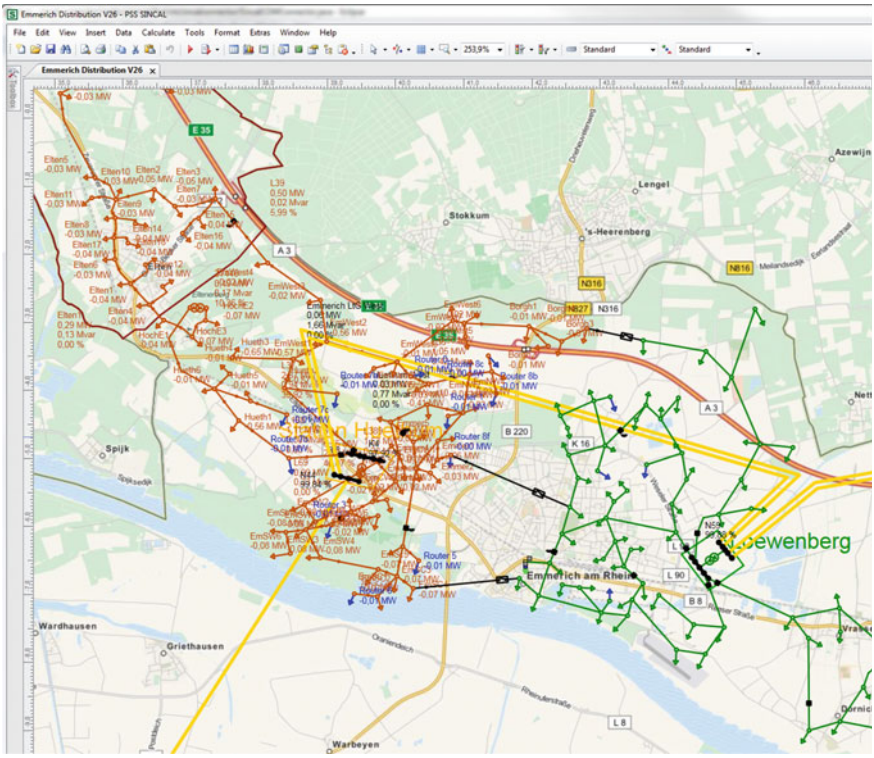


Fig. 8 Screenshot of the PSS®SINCAL software. The graphical user interface shows the elements of the distribution and transport network and their interconnections. The view can be enriched with geographical maps to support the modelling of real-world conditions

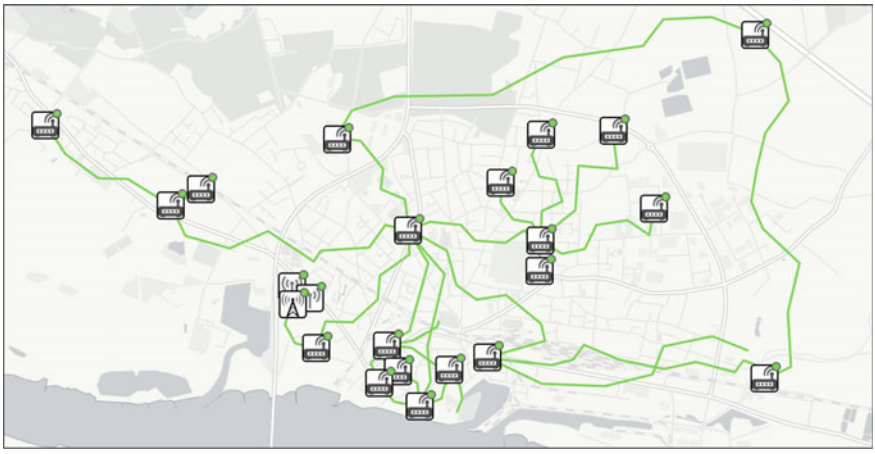


Fig. 9 Visualisation of the fictive telecommunication network within the city of Emmerich. Routers, mobile communication sending masts and telecommunication cables are depicted in an iconographic style

derailment scenario, where an important telecommunication cable gets destroyed during the simulated incident.

Compared to the electrical and telecommunication infrastructure, a number of publicly available data sources for the required modelling activities for the railway network could be used. We used information provided by the main German operator Deutsche Bahn and its daughter companies that are responsible for maintaining the railway network infrastructure. Other information was provided by DB Schenker, a logistics daughter of Deutsche Bahn, Keyrail, and others. Information on local railway traffic in the Emmerich area could be found on the mobility portal of the federal state of North Rhine-Westphalia (NRW) in Germany.

The model was built around the city of Emmerich, including parts the Netherlands and the Rhine-Ruhr area. The most important railway track in the scenario area is the Betuwe route, a double track freight railway from Rotterdam to Zevenaar, with extensions to Germany and the European hinterland (Rhine-Alps corridor of the railway network). It is an important European Infrastructure, as since 2011, nearly 80% of all goods trains between Rotterdam and the Dutch-German border took the Betuwe route. On the same route, also passenger trains are running, including international ICE lines. On the German side, the extension of the Betuwe route runs through the entire district of Kleve, with the city of Emmerich as the north-most station and the city of Wesel as the south-most. The part of the Betuwe route that runs through the incident region is the track between the cities of Arnhem (NL) and Emmerich (DE). Figure 10 shows an overview of the railway network covered by the simulation model.

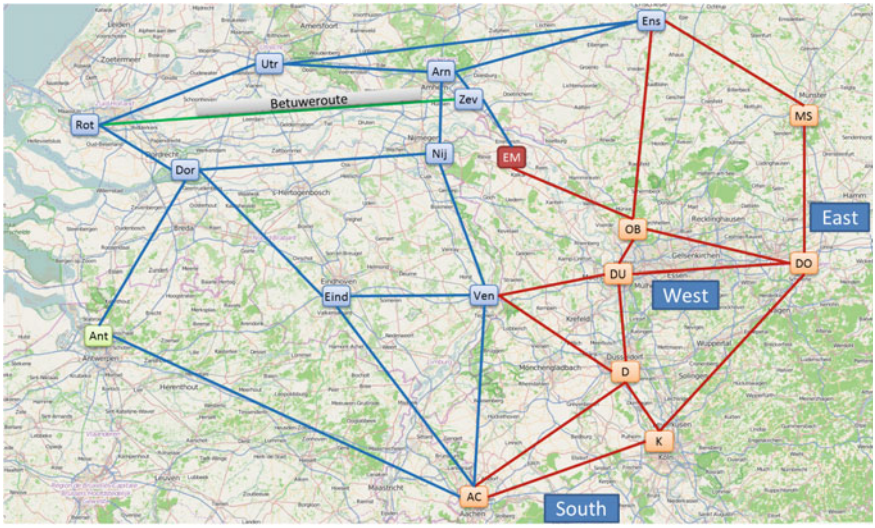


Fig. 10 The model of the main railway traffic lines from Rotterdam (Rot) to the German Ruhr region (OB, DU, DO) and further on southbound via Cologne (K). EM marks the city of Emmerich. Red connections depict railway lines in Germany, blue connections those in the Netherlands and Belgium

The model of the railway network in the OpenTrack software consists of the actual railway network, including tracks, stations and railway infrastructure like signals. Besides the railway network, the model includes the rolling stock data and the timetable information for each simulated train.

5.2.2 The Federated Simulation System

The interdependencies between individual CI simulators are implemented through the CEP engine of the CIPRTrainer software system. The dependencies between single infrastructure elements are described within the rule base of the CEP engine. Simplified, a rule describes a correlation in the form "if cabinet feeder X is inactive, router Y is inactive". The CEP engine is connected to the CI simulators through an event system. For each simulator involved in the federated simulation, a unified access layer to the basic simulator functions needed within the CIPRTrainer system is implemented, the so-called *Simulation Connector*. The simulation connectors provide access to the specific CI simulators used by the CIPRTrainer and implement functionality for the control of the simulators and for the retrieval of simulation data. As each simulator usually provides its own specific access mechanism, a dedicated simulation connector has to be implemented for each CI simulator used within the federated simulation environment. A schematic overview of a simulator connector is shown in Fig. 11.

Besides the common set of functionalities to implement the connection to the CEP engine, each simulator connector comprises a specialised connection module to the concrete simulator. As each CI simulator provides its own interface, this module has to be implemented for each simulator used within the federated simulation environment, while the common sub-modules can be reused for each new

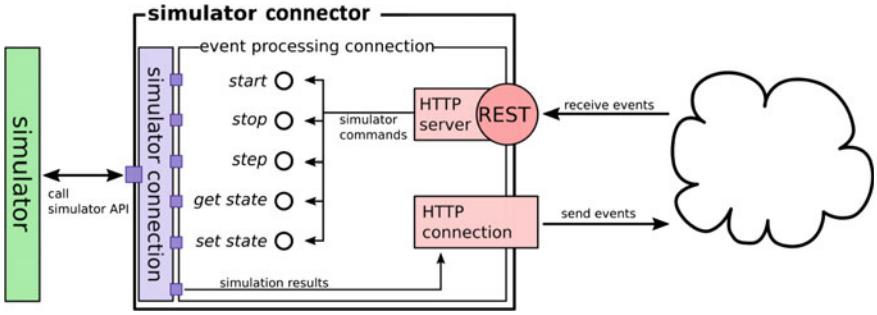


Fig. 11 Graphical overview of the simulation connector. Events are sent and received through the network via HTTP. A REST-based interface to the simulator commands is implemented through a HTTP server. CI element state changes as the outcome of a simulation are sent to the CEP engine using HTTP requests. The simulator connection sub-module realises the concrete connection to a specific simulator

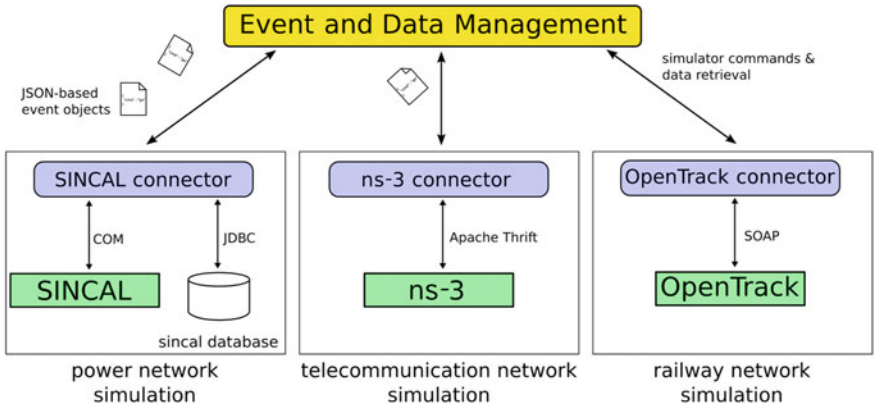


Fig. 12 The simulator connectors (*violet colour*) implemented for the CIPRTrainer with their connection to the specific simulators and to the CEP system (*green colour*)

simulation connector. In Fig. 12, an overview of the three CI simulators used in the CIPRTrainer software system, *PSS SINCAL*, *NS3* and *OpenTrack*, as well as their corresponding simulation connectors and the simulator-specific API (Application Programmer Interface) mechanisms are shown.

CIPRTrainer's what-if analysis functionality for CM training is based on the fast rollback of various simulated worlds. CIPRTrainer's different software components including the simulators (both domain-specific CI simulators and threat simulators), visualisation module, time management module and spatial objects support the rollback functionality. However, this functionality is implemented differently within the specific components. For the CI simulators, approaches like the adaption of the software versioning system git, or an internal implementation within the simulation connector are used. For other components like time management, visualisation and spatial information, the spatial-temporal features in the PostgreSQL database management system is used.

6 Impact and Consequence Analysis for the Global Assessment of Damages

In this section we will provide an introduction to the CA approach used in CIPRTrainer; explain which data we used; discuss issues in data acquisition, sanitation, and usage; explain how we displayed the results of CA in CIPRTrainer; discuss how the results should be interpreted.

6.1 Goal of the CA

The overall goal of the CA is to provide the CIPRTrainer users with the capability to understand the broader consequences of their action and inactions during and at the end of a training session. CA goes beyond impacts, as it clarifies the meaning of impacts and the inoperability of critical and non-CI for the population and businesses. A complete and detailed Ca of everything is not possible and not desirable. The CA therefore focuses on the CIPRTrainer user and the information he needs to learn and perform better than before. The CA module (CAM) of the CIPRTrainer is not intended to be a finished product readily usable for wide variety of conditions. Just like CIPRTrainer as a whole, it serves as a working demonstrator for the specified scenarios. But in general it should be possible to adapt the CAM to different scenarios. Therefore it needs to be conceptualised and implemented in a way that allows later modification.

6.2 General CA Concept

For the CAM we distinguish between impact and consequence. Impact is the direct outcome of an event, for example the destruction of a private house or the reduction/loss of function of an infrastructure. An impact has consequences, for example the rebuild cost of a private house or the economic losses due to the reduction/loss of the infrastructure function for infrastructure stakeholders. Impact can be differentiated in direct and indirect impacts. Direct impacts are the direct damages to CI elements or other assets. Indirect impacts are the cascading effects.

Consequences can also be differentiated into direct and indirect consequences. Direct consequences are directly related to the impact, for reconstruction cost of a flooded building. Indirect consequences are indirectly related to the impact, for example the number of homeless persons. A further differentiation is possible in CI related and other consequences. CI related consequences are related to the impacts of an incident on CI, for example the recovery costs for a CI operator, the GDP loss produced by a power outage or the number of households without electricity. Other consequences are related to the impacts on everything else, for example the re-construction cost of flooded houses. CA therefore comprises the estimation and assessment of these types of consequences of impacts.

6.3 Geographical Dimension of the Analysis

The CAM takes the geographical dimension of the impacts and consequences into account. For the CAM it is important where an impact has happened and where the consequences occur, which is not necessary the same area (cascading effects and

Fig. 13 Area of Emmerich with German 1 km × 1 km grid and power nodes and lines (OpenStreetMap)

indirect consequences). In the CAM we use two-dimensional grids to locate people and the built-up area (buildings, infrastructure and environmental areas). These grids are INSPIRE compliant.[2] For Germany we use a 1 km × 1 km grid (see Fig. 13), for the Netherlands a 500 m × 500 m grid, which are the standard grid sizes that these countries use.

For both grids census data from 2011 [26] is used, which comprises data on residents and residential buildings per grid cell. For German business data we had access to a derived spatial business dataset on street level. The data set was derived from different databases from commercial data providers:

- Deutsche Post Daten
- NAVTEQ (HERE)
- Microm consumer marketing

From the derived dataset we extracted the number of firms with specific NACE code on street level and allocated these firms to the grid.

[2]The INSPIRE directive (Infrastructure for Spatial Information in the European Community) aims to create a European Union (EU) spatial data infrastructure. This will enable the sharing of environmental spatial information among public sector organisations and better facilitate public access to spatial information across Europe http://inspire.ec.europa.eu/.

For data of land use we use CORINE land cover data from 2006 (see [27]), which are available free of charge. Infrastructure data with geographic coordinates could be derived from OpenStreetMap. It has to be mentioned that this data is far from complete as it depends on OSM users to insert the data sets. Some regions are more detailed than other regions. But for the purpose of CIPRTrainer it was sufficiently complete for the district of Emmerich.

For the use of grids in the CAM one important assumption was necessary: If a hazard has an impact on a grid cell, the whole grid cell is affected, e.g. if the cell is only partly flooded the assumption is that the whole cell is flooded. This assumption is necessary as we have no information about where in the cell the resident or buildings are located. This can lead to an overestimation of the consequences. With more detailed data it would be possible to relax this assumption.

6.4 Determining Impacts

The technical federate simulators are only able to provide impacts and cascading effects for their domain (electricity, telecommunication and train traffic) and the flood simulator does not produce any impacts by itself, it only calculates the geographical extent of the flood with attributes for height and rise rate. So we needed a separate impact module for the flood impacts and all other impacts of the different scenarios. It has to be noted that some impacts are not calculated; instead they are part of the storyline and therefore predefined. An example is the train derailment in the Emmerich Scenario, where the amount of damage to humans and buildings form the train crash is defined in the storyline.

Impacts on humans can lead to injuries and death. For operationalization mortality functions can be used. We based our approach on a general framework for loss of life estimation from Jonkman et al. [28]. Basis principle is to look at the exposed individuals to a certain hazard. If the people are informed they can shelter (i.e. keep the door and windows closed when a chemical cloud is coming, going upstairs in a flood etc.). They are exposed to the threat if they cannot shelter or self-evacuate themselves. Emergency forces can evacuate them if present (depends on trainee decision), otherwise they are exposed until the end of the threat. The effects of the impact on the exposed people are calculated with hazard specific mortality functions. The more intense an impact is (e.g. high flood depth and rise speed of water during a flood) the more casualties are to be expected. The inherent mobility of humans brings some conceptual issues. Usually residential data is used to assess impact on humans. But this leads to an overestimation of impacts on residential areas in the daytime, as normally a big part of the residents is at work (or school, university) or pursue other activities (shopping mall). There are different solutions discussed in the literature. More static approaches use a simplified binary distinction between daytime and night time distribution (see [29, 30]). Others try to develop models of dynamic behaviour of residents, which is a more difficult task (see [31]). Regarding CIPRTrainer scenarios the data available are not sufficient for

the dynamic modelling of the population. Then, a simplified approach is used considering only residential data.

The impacts on buildings, infrastructure elements and environment are conceptualised in a similar way to impacts on human. First these objects need to be physically exposed to a hazard, e.g. a house must be in the flooded area. Second the object must be vulnerable to the hazard. The damage depends of the intensity of the hazard (e.g. flood depth) and the degree of sensitivity of the object to the specific threat (e.g. the main material of the building: wood vs. brick). Some damage functions for specific threats and specific objects are available in the literature. For flooding we could draw upon the 'Standard Method 2004 Damage and Casualties Caused by Flooding' from the 'Ministerie van Verkeer en Waterstaat' [32] of the Netherlands and the book 'Hochwasserschäden' [33] for Germany. But not for all types of objects and hazards are damage functions readily available. In these cases we have made assumptions on the basis on available damage functions.

6.5 Evaluating Consequences

For the CA we decided to evaluate the consequences on humans only as the number of injuries and deaths. As an economic evaluation of life is impossible and would be a highly ethical issue, we refrained from doing so.

To assess the direct consequences on a specific building, infrastructure element or environmental area, we need a metric to express the value of the damage. We decided to use reconstruction cost for this purpose, because information about the potential reconstruction cost of residential, commercial, industrial and public buildings are derivable from official data on build cost in Germany and the Netherlands. For infrastructure elements and the environment the data is not readily available. So we had to rely on diverse pieces of information in different studies, surveys, books and websites to generate artificial data. To calculate the actual reconstruction cost for a specific object a damage factor is needed. This is conceptualised as a value between 0 and 1, with 0 no damage and 1 total destruction. This damage factor is determined by the impact module (e.g. flood-depth-functions). The actual reconstruction cost of a specific element is defined as a function of the damage factor. Figure 14 shows an example of a flood damage function for low-rise dwellings from [32].

For indirect economic consequences there are basically two major streams in economic theory: input-output models (IOM) and calculable general equilibrium models (CGE). Both modelling approaches address the interaction of the different economic sectors. They differ however in which manner these sectors interact and how the sectors react to external shocks [34, pp. 43–44, 35, pp. 116–118]. IO-models focus on the interrelations of production, where a sector needs inputs from other sectors to produce goods. In the basic IO-model prices don't play any role. On the other hand focus CGE models on the effects price variations to the supply and demand in the different sectors [34, p. 44]. The basic IO-model is demand driven. A disaster can therefore only be modelled as reduction of the final

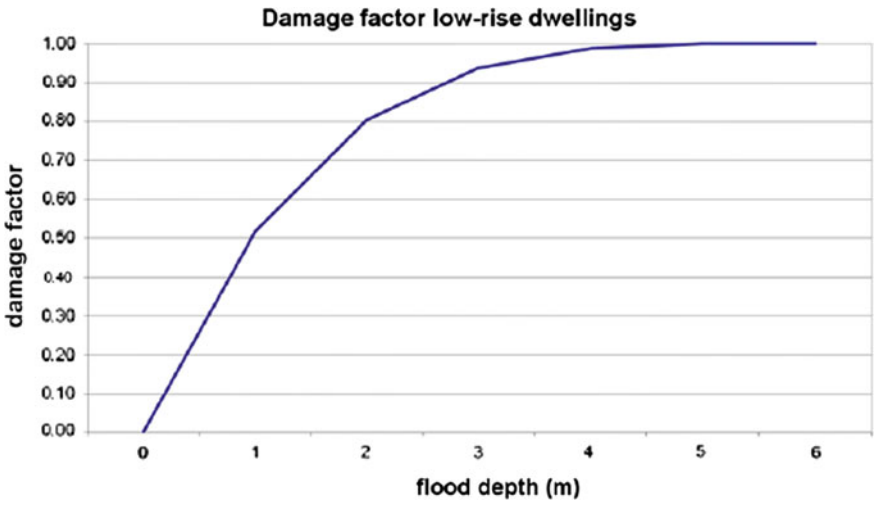


Fig. 14 Example of a flood damage function for low-rise dwellings [32]

demand. This causes a decrease in the production of final goods and subsequent in all dependent sectors who supply intermediate or raw goods for this final goods. A loss of production of a supplier firm due to a disaster has correspondingly to be modelled 'in reverse'. In newer IO-models this restriction has been relaxed. In contrast to IO-models there are no explicit flows of goods in a CGE model. The economic system is always perfect balanced due to the price mechanism of the markets. A reduction in production capital due to a disaster leads to a decrease of supply and a subsequently to a price increase. This leads in turn to a demand reduction and to a new equilibrium. Moreover, in CGE models production factors can be substituted in short term. This induces a fast adaption of firms to mitigate the disaster effects. CGE models are thus more optimistic than IO-models, where production technologies are fixed in the short term. One limitation of both approaches is the high aggregation level. Sectors are the main "economic actors". If one sector suffers from a disaster, all businesses aggregated in this sector suffer the same consequences, regardless of spatial location. There are no distinct production functions and no explicit supply chains modelled in the sector [34–36].

In the CAM the method of IOM is used to calculate the indirect effects of the disturbance of economic sectors in the CAM. In the course of time many variations and extensions of the basic IO-model were proposed in the literature (e.g. inoperability IOM [37, 38], supply driven IOM [39], but we decided to start with the basic model as it is the least data hungry and easiest to understand for the CIPRTrainer user. In the future an enhanced IOM could improve the explanatory power if needed.

One obstacle for the use of IOM in the CIPRTrainer is the lack of regional input-output data. There a proposals in the literature how to regionalise national data (see), but using one of these methods is a very complex and time consuming

task, hence not feasible in the timeframe of the CIPRNet project. Our approach was to assume that the regional input-output structure is the same as on the national level. The absolute values for the different sectors are proportional to the GDP share of the region. For the district 'Kreis Kleve' the GDP share was 1.3% of the national GDP in the year 2011. The IOM uses this 'regionalised' IO-table data.

Another obstacle is the lack of output data on business level, i.e. how much a business is producing in one year. We had to refer to a combination of value-added data on the district level and data on the number of firms with a specific NACE code in the district to generate a dataset on value-added per firm with a specific NACE code.

7 Using CIPRTrainer

CIPRTrainer is accessible through a regular Internet Browser. If all installation procedures are completed successfully, then the CIPRTrainer should be accessible on http://host-machine-ip/ciprtrainer. CIPRTrainer is a multi-user training system, which includes following user roles: trainees and trainer. Before a training session starts, the trainer prepares training scenarios for trainees. Whenever the trainer starts the scenario simulation, the pre-defined storyline will be executed and trainees can perform training. In the following, user roles, trainee and trainer modules will be described precisely.

7.1 User Roles

A study of the EU project PREDICT showed that although the CM governance structures in different countries vary to a great extent, there are some common roles of CM staff. CIPRTrainer supports the most essential of these roles. Typically, there are one or more persons responsible for collecting information on the situation ('situational awareness'). One or more persons are in charge of the CM ('decision taker' or commander or head of CM staff etc.). CM teams include people commanding the responders, like the head of the fire-fighters, head of police etc. ('operations'), and people heading municipal departments, like the head of the school department ('administration').

For this purpose, there are four different roles for trainees in CIPRTrainer: Situational awareness, operations coordinator, and administrative coordinator operate CIPRTrainer simultaneously. We called the latter two roles 'coordinator', since they combine functions that in reality would be assumed by more than one person. For pragmatic reasons and for feasibility, we restricted the number of simultaneous users to three (plus trainer). For each of the three roles, a specific set

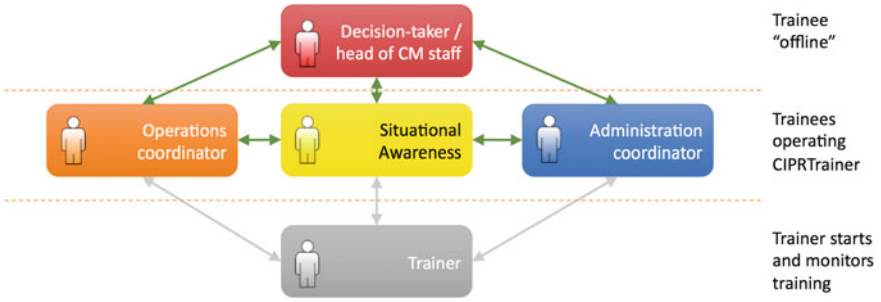


Fig. 15 Trainees and trainer user roles in CIPRTrainer

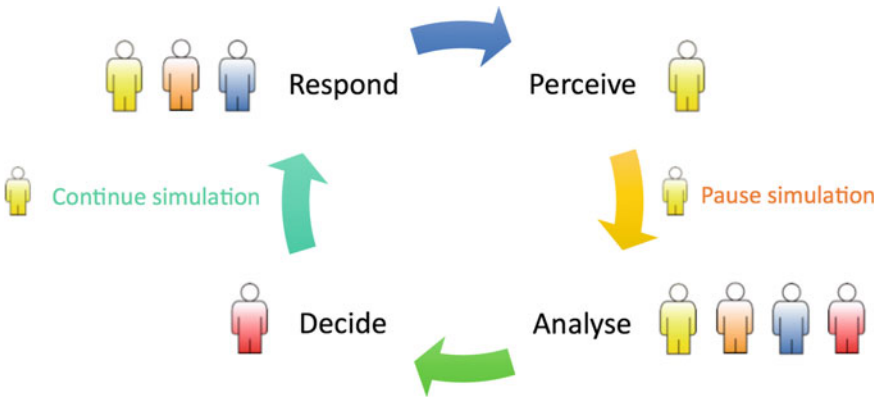


Fig. 16 CM cycle of perceiving, analysing, deciding, and responding. User roles in CIPRTrainer related to the phases of the cycle

of actions can be performed in simulation. A fourth trainee, the decision taker (or commander or head of CM staff), stays in the background (Fig. 15). CIPRNet has chosen this approach for supporting the wide applicability of CIPRTrainer.

The four trainees simulate the repeated CM cycle (Fig. 16) of situation update (perceive), situation analysis (analyse), decision taking (decide), action planning and execution (respond) [40]. The trainee acting as situation awareness staff member pauses the simulation for initiating the next cycle.

7.2 Trainee Module

Trainees have various options to interact with the system including:

- Pausing and continuing the scenario
- Performing various kind of actions (response, crisis management, administrative)
- Performing rollbacks (jumping into a prior state of the scenario)

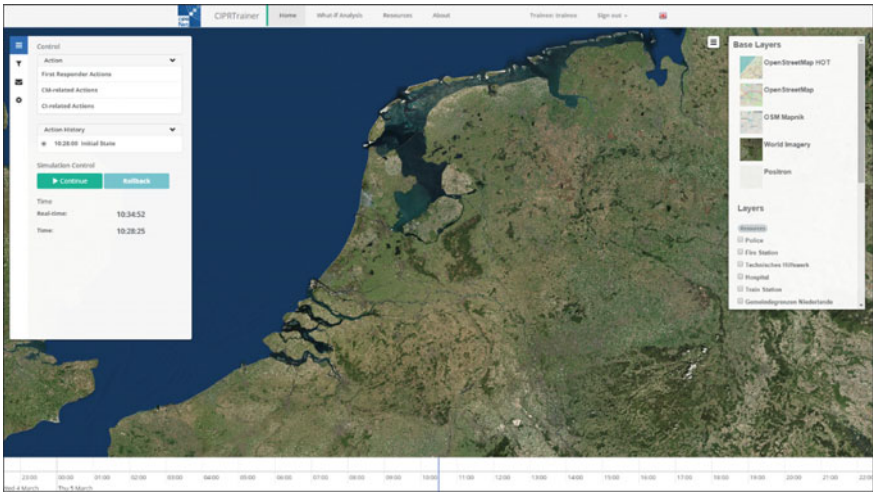


Fig. 17 Main view of CIPRTrainer UI for trainee consists of a navigation bar, two sidebars (*left* and *right*), a time-line (*bottom*) and a standard GIS map (*centre*). The *left* sidebar contains the *green* "Continue" button for resuming a paused simulation

- Examining and mapping CIs
- Observing and keeping track of the evolution of the scenario
- Customising CIPRTrainer view components (layer panels, timeline, etc.)
- Conducting CA
- Communicating with other participants

Pausing and continuing the scenario
On the left control panel of CIPRTrainer the user can click on the button Pause/Continue to pause or continue the scenario (Fig. 17). Other participants like trainees and trainer are notified when the scenario is paused or continued.

Performing various kind of actions (first responder and crisis management)
CIPRTrainer provides various kinds of actions including first responder and CM related actions. A user-specific list of actions is shown on the control panel. For instance, the operations coordinator is able to perform first responder related actions such as mobilising fire brigades and so on. In the following all actions are described in detail.

First Responder Actions incorporate resources like police, fire brigades and technical relief services (THW) and can be performed by operations coordinator (Fig. 18). The trainee can order different resources to perform an activity at a predefined location. Actual forces or resources are spread in the region around the scenario location (in this case Emmerich).

CIPRTrainer provides a map that depicts the different resources and their capacities. The capacities are presented as triple (leader, subleader and forces,

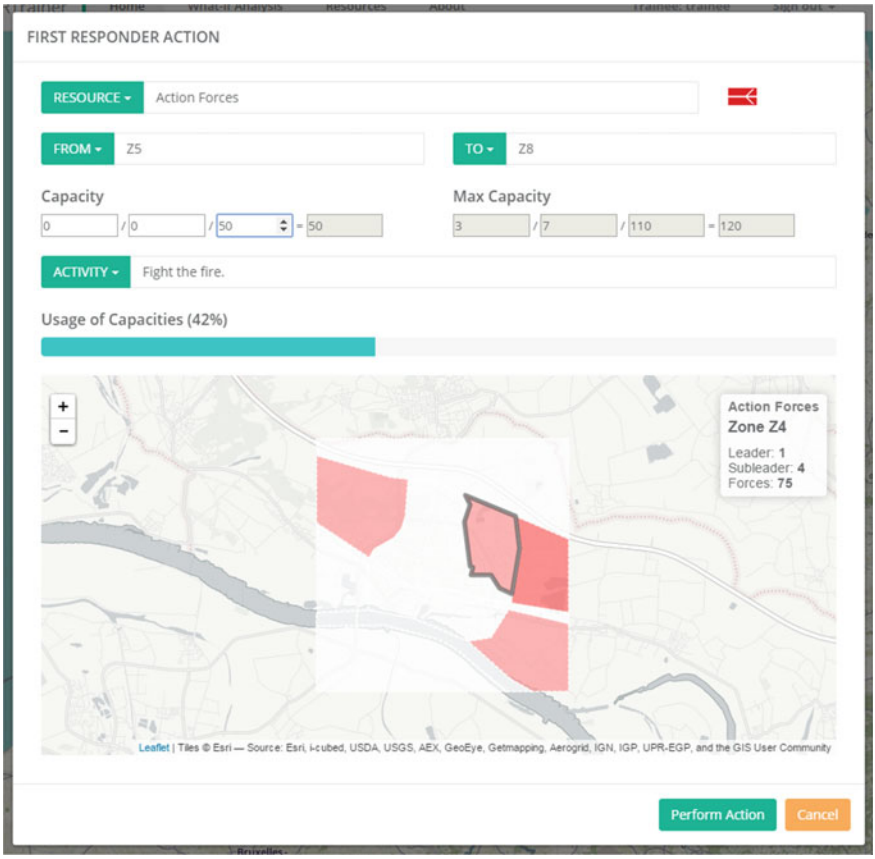


Fig. 18 Interface for performing first responder actions

see Fig. 19). The accumulation of these three values refers to the capacity strength of a specific unit. The user is able to send resources with a certain capacity to the crisis region. In addition to that, the trainee can select an activity that the forces perform in the crisis zone (e.g. fight the fire). Every participating trainee gets a notification whenever an action is performed (Fig. 18).

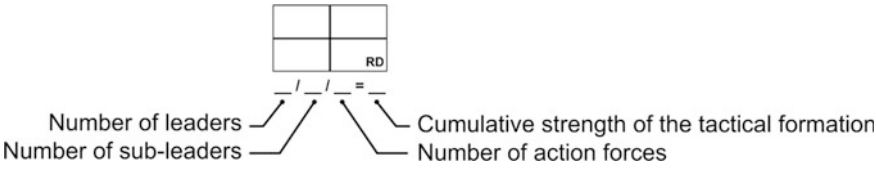


Fig. 19 Tactical symbol notation for strength details of units

CM actions are referred to as the second type of actions that CIPRTrainer provides. This type of actions can be performed by operations coordinator, administrator coordinator and the trainee who is responsible for the situational awareness. However, the actions between the trainees differ and are based on their decision-making authority. For instance, the trainee for situational awareness is able to alarm public authorities and the general public as well as request more emergency forces from other districts. Each action influences the consequences in the scenario. When the trainee decides to not inform the general public, the number of injured people will rise. On the other side, if the crisis manager performs this action in an early state of the scenario, then less people will be injured, which mitigates the consequences. Each action triggers predefined rules based on the action, the time and the underlying socio-economic data. The following lists available CM related actions for the different trainees.

Trainee for situational awareness:

- Request electricity power cut-off from electricity supplier in **<place>**
- Request locking the railroad track from train authorities
- Inform companies in the area that work with dangerous goods
- Contact European emergency response capacity
- Contact chief administrative officer of the district
- Request more emergency forces from other districts

Administration coordinator (see Fig. 20):

- Inform hospitals to prepare for casualties
- Prepare evacuation
- Support evacuation
- Inform the public by media (press, radio, television)
- Request support from municipal transport services for evacuation
- Block all critical bypass roads like tunnel and bridges

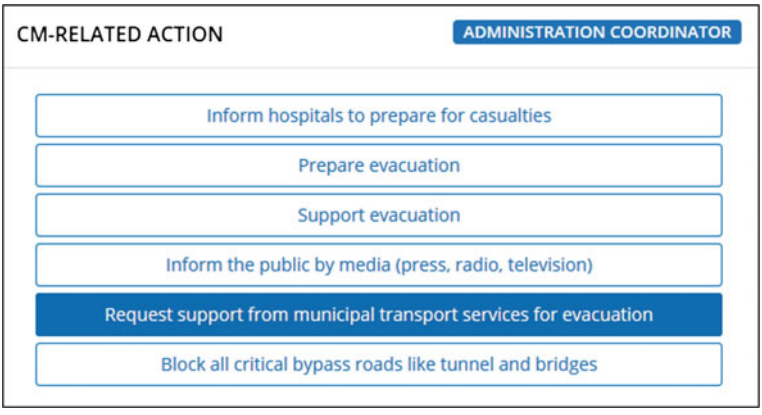


Fig. 20 Interface for performing CM actions by administration coordinator

The operations coordinator:

- Inform the public by sending action forces with speakers and sirens
- Fight fire
- Recover affected victims/humans
- Evacuate the accident site (initiate evacuation)
- Request special forces
- Block all critical bypass roads like tunnel and bridges
- Warn the public by using air raid sirens

Performing rollbacks (jumping into a prior state of the scenario)
To perform a rollback the user needs to decide first on which state the scenario should be reinstated. Therefore, CIPRTrainer adds every performed action in the Action History list. To perform a rollback the user needs to select an action in the Action History list and click on the button "Rollback". The scenario is then restored to the time the action has been performed.

Examining and mapping CIs
CIs can be examined using GIS overlays. The user is able to visualise and hide CI overlays by using the layer panel on the right side. To examine an entire CI model, for instance power networks, the user can click the list element highlighted with a grey background. By doing so, all components of a power network (e.g. cabins, substations, transformer, etc.) will be checked as well, and shown on the map. CI elements on the map are visualised using icons representing the entity with an underlying LED light on the upper right corner. This light indicates the operational status of the element. Table 1 shows the relation between colour and operational status of a CI element.

Observing and keeping track of the evolution of the scenario
The user has three options to observe and keep track of the evolution of scenario, namely using:

1. GIS map
2. Timeline
3. Notification Logs

Table 1 LED lights on the upper right corner of CI elements indicate the operational statuses

Colour	CI State
Green	Normal state; service up
Yellow	Service partially shut down; no substantial damages
Red	Service completely shut down due to damages
Blue	Service completely shut down, but currently no damages

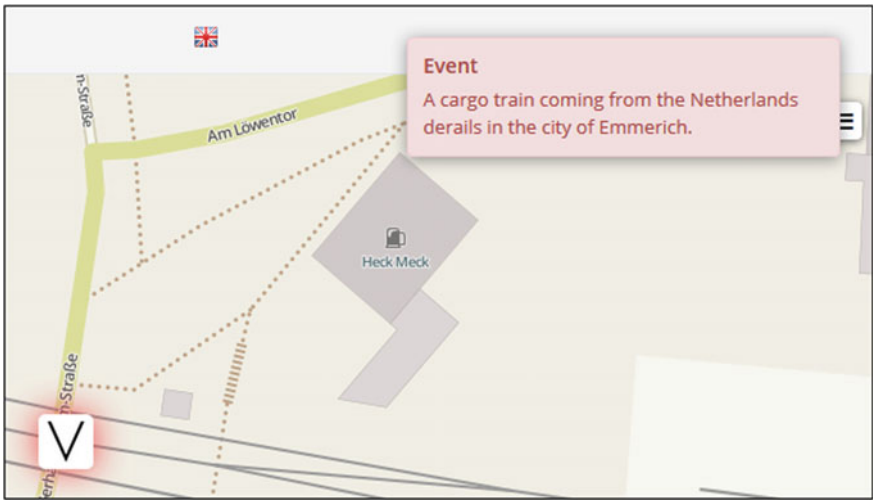


Fig. 21 Event notification label on the *upper right corner* depicts a short summery of the event

CIPRTrainer GIS map visualises storyline events and status reports as GIS elements using the corresponding tactical symbol on the map. When CIPRTrainer receives an event by the Scenario Executor, the team will get a notification showing up on the upper right corner containing a short description of the event. Simultaneously, the event appears on the map, too (Fig. 21).

Clicking on the item reveals a pop-window with more detailed information showing a short description and accident time (Fig. 22). To gain more information, the user can click on the 'Read More' button. A new window pops up including all information of this event (Fig. 23). To close the window pop-up, the user can push key ESC or click outside the message box. To hide the all events on the map, the user can toggle the list element 'Critical Events' on the layer panel.

The CIPRTrainer timeline (Fig. 24) shows various kinds of events in a chronological order. Different event types have different colours (Table 2). To know more about the event, the user can click on the label. A window pop-up shows up and can be closed by pushing the key ESC or click outside of the window.

Managing user account and customising CIPRTrainer view components

The trainee can change first name, last name, email address and password in the settings panel. To customise CIPRTrainer, the user is can show or hide certain UI components by checking or uncheck the desired component on the list, respectively. Following components are listed:

1. Base Layers
2. Layers
3. Timeline

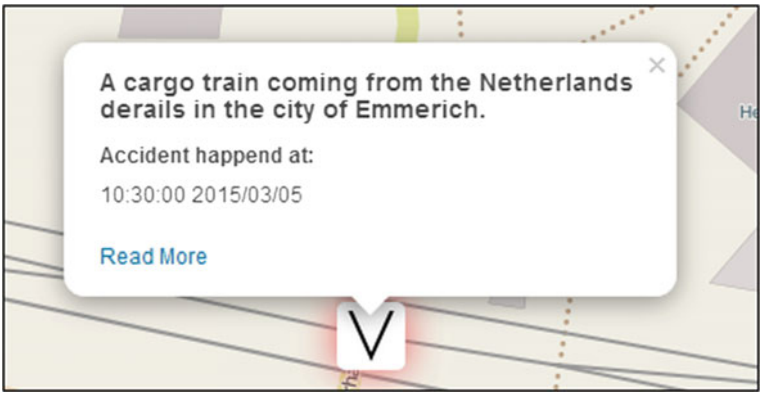


Fig. 22 Information panel of a GIS element appears by clicking on it

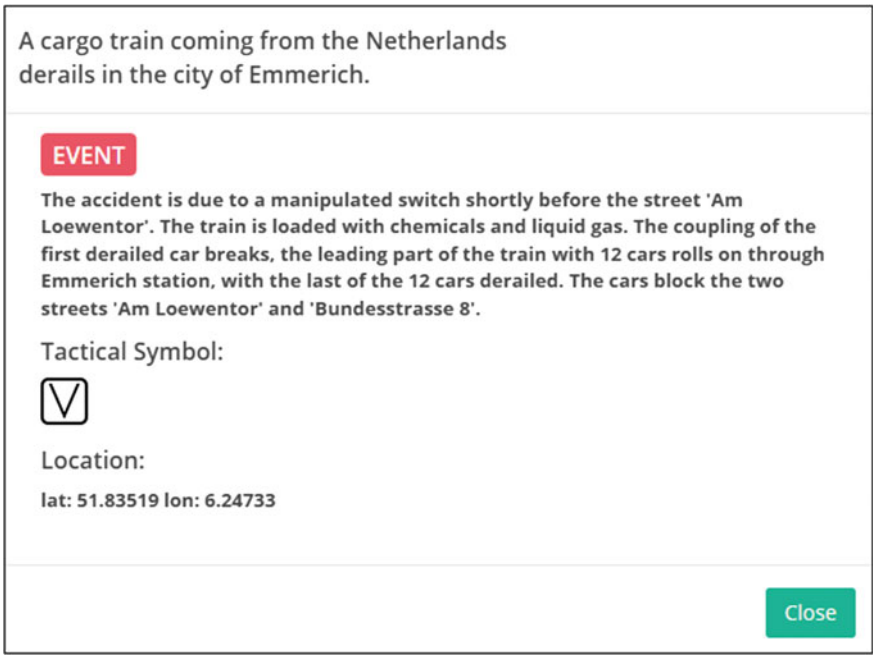


Fig. 23 Window panel containing all information shows up by clicking on the element on the timeline or "Read me" button

Conducting CA

For using the CAM, the team can click on the button 'What-if Analysis' on the navigation bar. The first section contains information about performed actions and rollbacks. The graph is an n-dimensional tree containing x nodes, where n reflects

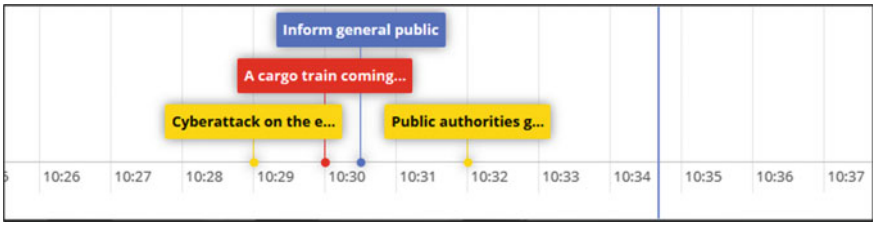


Fig. 24 Timeline depicting various types of events

Table 2 CIPRTrainer incorporates various types of events: action events, events defined in the SDL, events produced by the federated simulators and general non-georeferenced events

Event Type	Colour	Location
Action events (performed by trainee)	blue	Partially
Events defined in the scenario	red	Yes
Events produced by the federated simulation	red	Partially
Non-georeferenced events and other events	yellow	No

the number of performed rollbacks and $x - 1$ the number of performed actions. The start node (marked as yellow in Fig. 25) illustrates the initial state of the scenario. Green nodes represent final actions, on which CAM can be performed. To examine the graph, the trainee can click on the nodes to read more details about the actions and use the navigation controls of the network panel.

Please note, whenever the what-if analysis view is active the simulation automatically pauses, if it was running, or remains in the state stopped, if trainer stopped the simulation before. To conduct the CA, the trainee can click the button "Acquire CA Results". Several computation processes are started in the backend. CIPRTrainer shows CAM results using:

1. Tables
2. Diagrams
3. GIS map

The tables contain information about various kinds of damages without geospatial context (Fig. 26), whereas the GIS map depicts several spatial-related results using colour schemes to support map diagnostics (Fig. 28). Diagrams are used to compare training results (Fig. 27).

The trainer's main tasks are choosing, starting and stopping scenario, and acquiring CA results and training protocol. Therefore, CIPRTrainer provides a

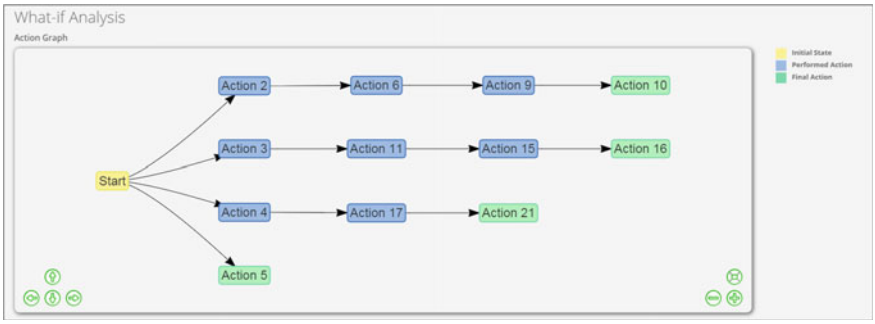


Fig. 25 Example of action graph. Each node of the n-dimensional tree refers to an action. The rollback capability creates an additional branch, on which following actions can be added. Final actions are marked as *green* nodes. The root node corresponds to the initial state of the scenario. In this example, the end-user performed four rollbacks

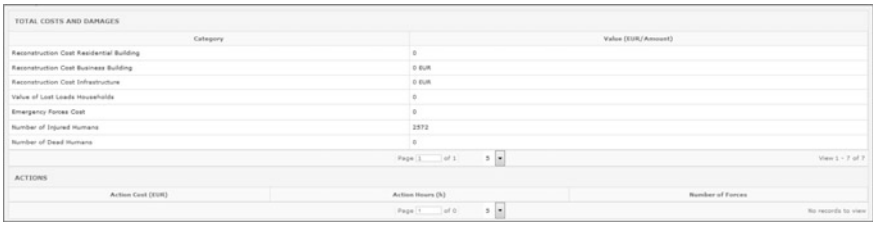


Fig. 26 CA table showing CA results that are non-spatial

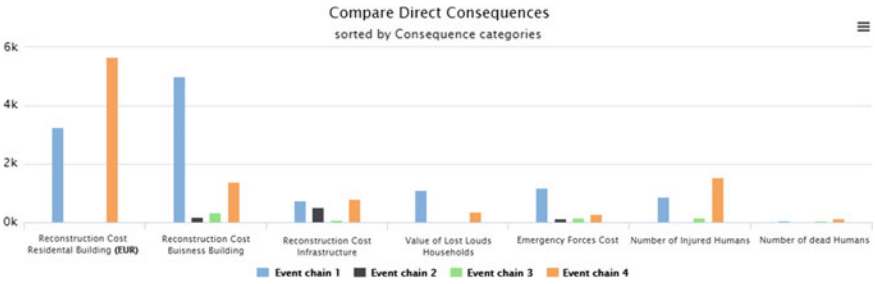


Fig. 27 CA diagram showing four different training sets

dashboard that includes all important information for performing the major tasks (Fig. 29). The dashboard includes:

- List of possible scenarios to train with
- Scenario status (paused, continued), simulation time and real time
- Online/offline status of the participants

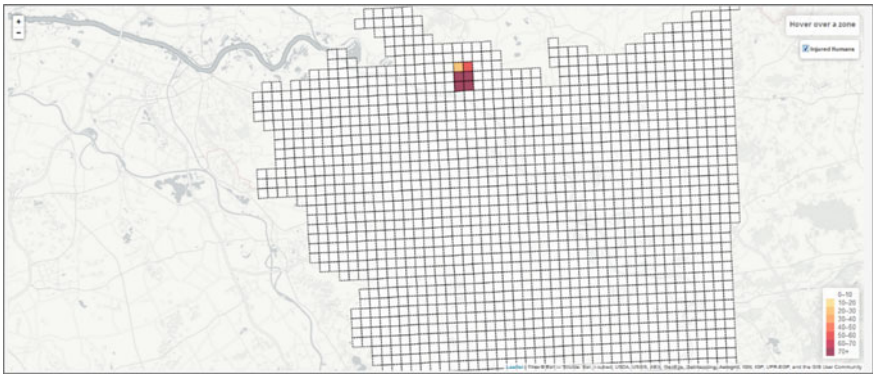


Fig. 28 GIS map showing spatial results

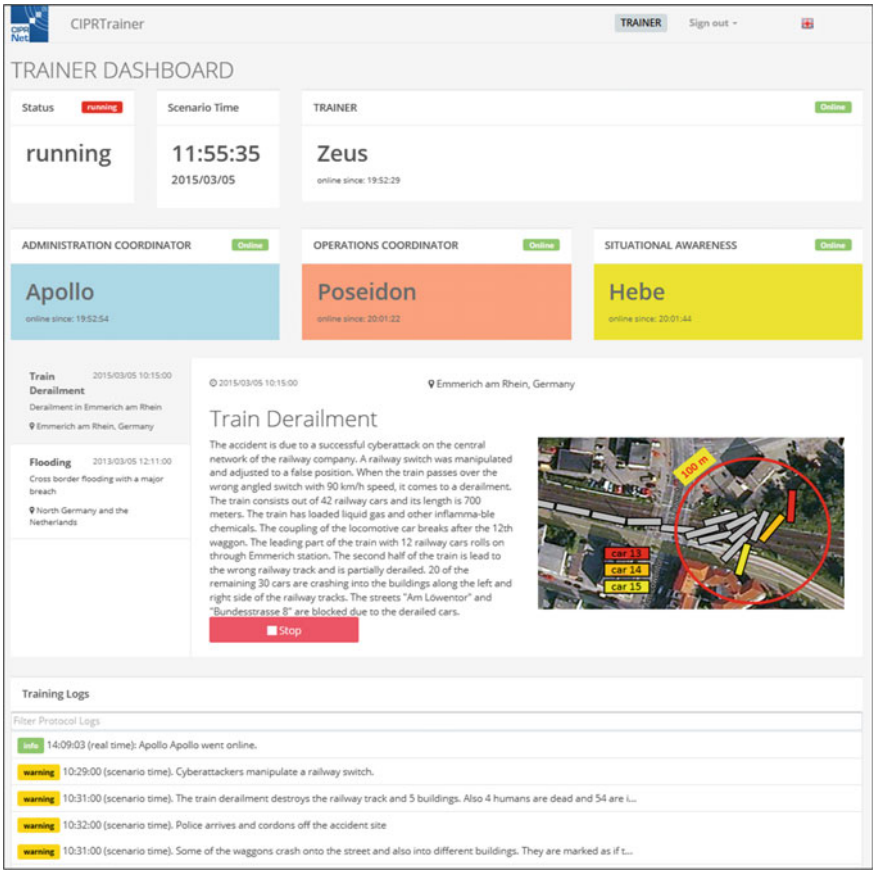


Fig. 29 The trainer dashboard contains information about the running scenario, the statuses of the participants, a list of possible scenarios, of which the trainer can choose one to run; control functions for starting and stopping the scenario, and the possibility to download results of the CA and training logs

- List of training logs including trainees interactions with the system
- Download panel for acquiring training analysis results

Setting up the scenario
Trainer can choose a scenario from the scenario list. By clicking on the item, a description of the scenario will show up and a button for starting or stopping the simulation. The button can only be activated when the team is complete.

Download results
For downloading the CA results and training logs, the trainer can navigate to the download panel and click on "Download All" to acquire a single JSON file with both CA results and training logs.

8 Example of a Training Session

In this section we will briefly describe the train derailment scenario storyline; describe what actions a trainee could perform; what critical decision points the scenario contains; explain how one anonymous trainee used the system; explain which what-if actions the trainee performed; explain what insights were gained in that session.

In the train derailment storyline, we assume a sudden derailment of a cargo train in the city centre of Emmerich am Rhein, caused by a malfunctioning switch point due to a cyber-attack on the electronic railway control centre Emmerich. Fire, spilled chemicals and a toxic gas cloud affect citizens, built infrastructure and CIs. The immediate impacts of the crisis take place within a few hours, while the remedy of the impacts takes days and weeks. The scenario consists out of a sequence of events that simulates the different stages of an accident that leads to the destruction of components. The different events require actions that are supposed to minimise the expansion of destruction and injuries.

The scenario is initiated with a cyber-attack event that manipulates a railway switch near the control centre in Emmerich. This manipulation leads to a derailment of a cargo train that has cars loaded with chemicals and liquid gas. Those cars crash onto the street and also into different buildings. After this accident happens the information is published through different channels. At first the train conductor informs the railway control station and in parallel the general public inform the police and fire brigade. Since Emmerich is quite small the police arrives contemporary and starts to cordon off the accident site. Also the mayor officially calls the disaster event.

Until this point the CIPRTrainer trainee user was not able to interact with the scenario storyline. Now the user is able to select different actions that may support the operation and lead to less destruction and injuries within the scenario. The following lists some of the available actions:

- Send action forces/rescue forces/law forces from <location> to <location>
- Inform the public by media (press, radio, television)
- Inform the public by sending action forces with speakers and sirens
- Inform hospitals to prepare for casualties
- Cordon off the scene of accident
- Recover affected victims/humans
- Evacuate the accident site
- Evacuate population from <location> to <location>
- Request special forces
- Request locking the railroad track from train authorities
- Inform companies in the area that work with dangerous goods
- Block all critical bypass roads like tunnel and bridges
- Request more emergency forces from other districts.

Most of the actions are generic and only few actions need a parameter for the location from where the resources are taken and assigned to. First thing that would be expected by the trainee is to act accordingly to the recommend disaster principal actions: danger recognition, cordon off the area, recover victims and request appropriate Special Forces.

The next storyline event that influences the disaster area are chemicals flowing out from the railway cars and ignite in the middle of the street near several buildings. It destroys the area around the accident location and part of the railway tracks infrastructure. There is an imminent risk of further explosions of chemicals. A toxic gas cloud emerges from the fire and the wind blows it in north-eastern direction. In between the railway control station switched off the power from the overhead electricity, this allows fire-fighting operations in the centre of the disaster area. At this time an additional railway car that was loaded with liquid gas explodes. Because of this, nearby buildings get destroyed, chemicals flow into the sewer system and ignite. Power lines inside the sewer systems are destroyed as well as telecommunication components. The toxic gas cloud diffuses in the area of Emmerich and affects humans and businesses. The Rhein-Waal Terminal in the port of Emmerich has to stop working and the harbour is inoperable.

While all these events appear inside the CIPRTrainer GUI the trainee is able to execute actions. Some of the destruction events can be avoided by executing the appropriate actions that obviate further destructions. For instance the destruction of power lines and telecommunication components inside the sewer system can be avoided by sending enough fire forces to the disaster location. In case that the trainee send 30 or more fire-fighter, the explosion of the railway car can be avoided and the subsequent destruction events will not occur. The toxic gas cloud requires a wide-spread evacuation and information action so contamination of humans can be reduced.

The what-if analysis enables the trainee to try different courses of action in the scenario during a training session. The underlying concepts are ‘rollback’ and ‘consequence analysis’, which have been described before in detail. During the training the trainee can request the CA and get the results for the current training branch. After that he rollback to a former time point in the simulation, try out

different actions and request once again the CA. This enables him to compare the different outcomes of the incident evolution and his own actions. In our example the trainee could compare the results of sending different numbers of fire-fighters to the hotspots in the scenario.

After the training the trainer can give feedback to trainee about his performance during the training. Besides the result comparison, the trainee can learn how he reacts under uncertainty and time pressure. In contrast to real-world crisis the trainee can learn from trial and error, due to the what-if analysis capabilities of CIPRTrainer.

9 Outlook

CIPRTrainer provides new advanced training capabilities to crisis managers for decision-making in crisis situations. What-if analysis and CA implemented in CIPRTrainer provide a comprehensive solution for scenario-driven CM training. Despite the sophisticated functionalities provided in CIPRTrainer, there is still room for improving it such that it better meets the needs of CM training.

- Multi-user training support will be improved to enable a better collaborative training experience.
- A community-driven European scenario database (ESDB) built on top of the Scenario Description Language SDL will be developed. Combining CIPRTrainer with ESDB will provide a large set of training options for different crisis scenarios.
- Decoupling simulators from the CIPRTrainer core engine. Other organisations and institutions will be able to plug-in their own simulators. The open communication interface will be published, so that third-party simulator providers can use CIPRTrainer as a training platform, which uses the simulators during the training session. Use CIPRTrainer as a kind of cloud-based training for crisis management.
- Advanced visualisation of the CAM is currently under development and will be available in the future release.
- To deploy the system on other sites, a significant amount of efforts and know-how is still needed. Easy deployment with container-based solutions like Docker will be integrated. Due to data privacy and security, cloud-based solutions are not optimal.

Moreover, the limitation of syntactic checking will remain for the time being. Semantic checks are an option for the future work. Extensions of the federated simulation system would require the development of connectors if new simulators need to be added. This is a design feature of the way we implemented federated

simulation (cf. also [DIESIS]). Developing new connectors requires a deep understanding of the RESTful interfaces and the simulator interfaces.

To maximise system performance, several functionalities will be moved into the database management system as extensions to avoid the overhead of network transmission of data, similar to what has already been done in the CAM. Validating SDL including rules and other scenario elements on a semantic level is a challenging task and formal ontology with dedicated Description Logic reasoners can facilitate this task. Impacts and consequences are in fact a function of time, i.e. they change as time evolves. This issue could be addressed as well in future versions of CIPRTrainer. Reusability of several components in CIPRTrainer is a long-term goal, especially reusing the CM scenarios encoded in SDL, as a kind of European scenario database, and the federated simulation environment, as the proposed EISAC, for other similar research projects and even production environments.

10 Conclusion

This chapter presented a comprehensive description of CIPRTrainer, an innovative application designed for CM training. CIPRTrainer provides the novel capability of what-if analysis for exploring different courses of actions in complex simulated crisis scenarios involving CI. A trainee that uses CIPRTrainer can 'go back in time', revert a decision, and can choose a different course of action. This is possible in simulation, but not in reality. For comparing the consequences of the scenario evolution and assessing the outcomes of the chosen courses of action, CIPRTrainer uses Consequence Analysis methods. Federated simulation of CI provides information on disaster impacts like CI outages and resulting cascading effects.

The realisation of this new what-if analysis capability is based on several core technologies and innovative methods. CIPRTrainer's core building blocks that are essential for providing the functionalities are:

- ***Scenario management***. It includes the creation, conversion and execution of CI-centric CM scenarios with an emphasis on dependency modelling of CI. Scenarios are created within SyMo in an offline fashion. The results can be exported as SDL, which is the Scenario Description Language developed for modelling CM scenarios. Scenario Executor, which is part of the scenario management components, can import and execute SDL.
- ***Declarative dependency handling with Complex Event Processing***. Cascading effects caused by sophisticated dependencies between CI are deduced by executing the declarative rules encoded in EPL—Event Processing Language. The open source event-processing engine Esper has been adopted to interpret the rules. It has been seamlessly integrated into the CIPRTrainer backend.

- ***Federated simulation system with models, simulators and connectors***. It provides the technical basis for performing rollback and what-if Analysis, since in real-world context rollback of what has already happened is not possible. The simulation backend consists of three domain-specific CI simulators—SINCAL, ns-3 and OpenTrack—plus one threat simulator, the flooding simulator. For each simulator, a CIPRTrainer connector has been developed, enabling the RESTful communication with other components.
- ***Consequence Analysis***. CM involves performing various kinds of user actions like initiate an evacuation under crisis situations, send a unit of first responders (police, fire fighters, medical emergency services, etc.) to a certain location, etc. The impacts and consequences of performing these actions are provided by this module. Technically, it is implemented inside of the database management systems to maximise the system performance.
- ***HTML5 Web front-end for interaction with system users***. Advanced Web technologies are adopted to provide a pervasive user experience. This includes responsive design that enables an optimal 'Look and Feel' with different browser configuration and mobile devices. HTTP Push technology minimise the delay of event visualisation by avoiding constantly queries the CIPRTrainer backend. In addition, an internationalised user interface makes CIPRTrainer useful for cross-border scenarios.

From the technical point of view, all these components are loosely coupled with RESTful Web services with a high-level of scalability—in terms of both development productivity and system running performance.

Besides the technical implementation of the CIPRTrainer software system, there were two more major challenges in the design and realisation. One was the modelling activity for creating complex and realistic scenarios, and the other was designing the user interaction in a way that makes CIPRTrainer usable for training in a wider range of countries.

The modelling of the complex scenarios was a heterogeneous activity covering roughly three different aspects: (1) Static modelling for creating an ontology of elements to be considered, including resources, crisis management actions, threats, and more; (2) impact and damage modelling for consequence analysis; and (3) models of interconnected CI. For all these modelling activities, data needed to be acquired. When such data were missing, plausible artificial models, e.g. for electricity distribution networks, needed to be created with help from domain experts.

The model of the user interaction was guided by analysis of the crisis management governance structure in several European countries. Though these structure were sometimes vastly different, it is possible to identify common roles in several CM governances. These include decision-taking (or command), situational awareness, response leaders and leaders of administrative departments.

So far, CIPRTrainer has been demonstrated several times, and has also been used for two training exercises at the Master of Homeland Security study at Università Campus Bio-Medico di Roma and at the Fraunhofer campus in Sankt Augustin, Germany.

Acknowledgement and Disclaimer This chapter was derived from the FP7 project CIPRNet, which has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no. 312450.

The contents of this chapter do not necessarily reflect the official opinion of the European Union. Responsibility for the information and views expressed herein lies entirely with the author(s).

References

1. Luiijf E, Klaver MHA (2009) Insufficient situational awareness about critical infrastructures by emergency management. In: Symposium on C3I for crisis, emergency and consequence management IST-086/RSY-019, May 2009, Bucharest, Romania, NATO Research and Technology Organisation, RTO-MP-IST-086, paper 10. http://www.rta.nato.int/pubs/rdp.asp?RDP=RTO-MP-IST-086, 10 p
2. Klaver MHA, Luiijf HAM, Nieuwenhuijs AN, Van Os N, Oskam V (2016) Critical infrastructure assessment by emergency management. In: Rome E, Theocharidou M, Wolthusen SD (eds) Critical information infrastructures security, 10th international workshop, CRITIS 2015, Berlin, lecture notes in computer science, vol 9578. Springer, Heidelberg, pp 79–90
3. Barrett C, Beckman R, Channakeshava K, Huang F, Kumar V, Marathe A, Marathe M, Pei G (2010) Cascading failures in multiple infrastructures: from transportation to communication network. In: 5th international conference on critical infrastructure (CRIS), pp 1–8
4. Petermann T, Bradke H, Lüllmann A, Poetzsch M, Riehm U (2010) Gefährdung und Verletzbarkeit moderner Gesellschaften – am Beispiel eines großräumigen Ausfalls der Stromversorgung. Endbericht zum TA-Projekt. Hg. v. TAB (141)
5. Luiijf E, Klaver M (2005) Critical infrastructure awareness required by civil emergency planning. In: Proceedings of the 2005 first IEEE international workshop on critical infrastructure protection (IWCIP'05). IEEE, p 8f
6. Deutch D, Ives ZG, Milo T, Tannen V (2013) Caravan: provisioning for what-if analysis. In: CIDR, 2013
7. Lakshmanan LVS, Russakovsky A, Sashikanth V (2008) What-if OLAP queries with changing dimensions. In: IEEE 24th international conference on data engineering, 2008 (ICDE 2008), pp 1334–1336, April 2008
8. Golfarelli M, Rizzi S, Proli A (2006) Designing what-if analysis: towards a methodology. In: Proceedings of the 9th ACM international workshop on data warehousing and OLAP. ACM, pp 51–58
9. Chaudhuri S, Narasayya V (1998) Autoadmin "what-if" index analysis utility. In: Proceedings of the 1998 ACM SIGMOD international conference on management of data, SIGMOD'98, New York, NY, USA. ACM, pp 367–378
10. Haas PJ, Maglio PP, Selinger PG, Tan WC (2011) Data is dead… without what-if models. PVLDB 4(12):1486–1489
11. Cai Z, Vagena Z, Perez L, Arumugam S, Haas PJ, Jermaine C (2013) Simulation of database-valued markov chains using SimSQL. In: Proceedings of the 2013 ACM SIGMOD international conference on management of data, SIGMOD'13, New York, NY, USA. ACM, pp 637–648
12. Dalvi N, Ré C, Suciu D (2009) Probabilistic databases: diamonds in the dirt. Commun ACM 52(7):86–94
13. Huang J et al (2009) MayBMS: a probabilistic database management system. In: Proceedings of the 2009 ACM SIGMOD international conference on management of data. ACM
14. Rome E, Langeslag P, Usov A (2014) Federated modelling and simulation for critical infrastructure protection. In: D'Agostino G, Scala A (eds) Network of networks: the last frontier of complexity. Springer, Cham, Heidelberg

15. Xie J, Theocharidou M, Barbarin, Y, Rome E (2016) Knowledge-driven scenario development for critical infrastructure protection. In: Rome E, Theocharidou M, Wolthusen SD (eds) Critical information infrastructures security, 10th international workshop, CRITIS 2015, Berlin. Lecture notes in computer science, vol 9578. Springer, Heidelberg, pp 91–102
16. EU FP7 CIPRNet, CEA, Deliverable D6.2—Application Scenario. Gramat, France, 2014
17. EU FP7 CIPRNet, Fraunhofer, Deliverable D6.3—Federate CI Models. Sankt Augustin, Germany, 2015
18. EU FP7 CIPRNet, Fraunhofer, Deliverable D6.4—Implementation and integration of the federated and distributed cross-sector and threat simulator. Sankt Augustin, Germany, 2016
19. Sojeva B (2015) Using Web GIS for designing added-value training systems for crisis managers. Master's thesis, University Koblenz-Landau, Germany
20. Nieuwenhuijs A, Luiijf E, Klaver M (2008) Modeling dependencies in critical infrastructures. In: Goetz E, Shenoi S (eds) Critical infrastructure protection, IFIP Series, vol 253, pp 205–214
21. Rinaldi S, Peerenboom J, Kelly T (2001) Identifying, understanding and analyzing critical infrastructure interdependencies. IEEE Control Syst Mag 21(6):11–25
22. Rinaldi S (2004) Modeling and simulating critical infrastructures and their interdependencies. In: 37th Hawaii international conference on system sciences, vol 2, USA. IEEE
23. The SIEMENS PSS® SINCAL Home Page http://www.sincal.de (last access on 16/07/2015)
24. ns-3 home page http://www.nsnam.org (last access on 16/07/2015)
25. The OpenTrack Home Page http://www.opentrack.ch (last access on 16/07/2015)
26. European Commission (EUROSTAT) (2014) The census hub: easy and flexible access to European census data. doi:10.2785/52653. ISBN 978-92-79-37803-4. http://ec.europa.eu/eurostat/de/web/population-and-housing-census/census-data/2011-census
27. CORINE Land Cover (CLC2006); Federal Environment Agency, DLR-DFD 2009
28. Jonkman SN, Lentz A, Vrijling JK (2010) A general approach for the estimation of loss of life due to natural and technological disasters. Reliab Eng Syst Saf 95(11):1123–1133. doi:10.1016/j.ress.2010.06.019
29. Freire S, Aubrecht C (2012) Integrating population dynamics into mapping human exposure to seismic hazard. Nat Hazards Earth Syst Sci 12(11):3533–3543
30. Leung S, Martin D, Cockings S (2010) Linking UK public geospatial data to build 24/7 space-time specific population surface models. In: GIScience 2010: sixth international conference on geographic information science. University of Zürich, Zurich
31. Polese M et al (2014) CRISMA. Version 2 of dynamic vulnerability functions, systemic vulnerability, and social vulnerability. Deliverable D4.32, CRISMA-Project
32. Kok M, Huizinga H, Vrouwenvelder A, Barendregt A (2005) Standard method 2004 damage and casualties caused by flooding. DWW-2005-009. Ministerie van Verkeer en Waterstaat
33. Thieken AH (ed) (2010) Hochwasserschäden. Erfassung, Abschätzung und Vermeidung. Oekom, München
34. Hallegatte S (2014) Natural disasters and climate change. An economic perspective, Chapter 2. Springer, Berlin
35. Okuyama Y (2007) Economic modeling for disaster impact analysis: past, present, and future. Econ Syst Res 19(2):115–124. doi:10.1080/09535310701328435
36. Rose A (1995) Input-output economics and computable general equilibrium models. Struct Change Econ Dyn 6:295–304
37. Lian C, Haimes YY (2006) Managing the risk of terrorism to interdependent infrastructure systems through the dynamic inoperability input–output model. Syst Eng 9(3):241–258. doi:10.1002/sys.20051
38. Santos JR, Haimes YY (2004) Modeling the demand reduction input-output (I-O) inoperability due to terrorism of interconnected infrastructures. Risk Anal 24(6):1437–1451. doi:10.1111/j.0272-4332.2004.00540.x

39. Smith BJ, Vugrinm ED, Loose VW, Warren DE, Vargas VN (2010) An input-output procedure for calculating economy-wide economic impacts in supply chains using homeland security consequence analysis tools. In: Proposed for presentation at the North American regional science council 57th annual North American meetings of the regional science held 10–13 Nov 2010. Sandia National Laboratories
40. Karsten A (2014) Führen durch die Chaos-Phase. Bevölkerungsschutz 4(2014). Themenheft "Kritische Infrastrukturen". BBK, Bonn, pp 32–35. ISSN 0940-7154

Chapter 11
Model Coupling with OpenMI Introduction of Basic Concepts

Bernhard Becker and Andreas Burzel

Abstract Interaction processes between two or more model domains can be represented with the help of model coupling. Different methods of coupling apply for different interaction processes. We illustrate this with the help of an exercise. In order to facilitate model coupling of water-related models the OpenMI standard has been developed. This document gives an introduction to the open modelling interface (OpenMI) and explains the steps that are necessary to migrate existing model code to Open MI compliance. An OpenMI composition of a flow simulation model for a river section of the Elbe river (Germany) that is coupled with a model for the control of a hydraulic structure is used to explain how models can be coupled with Open MI and to illustrate the added value of model coupling in terms of improved simulation result.

1 Introduction

This document is accompanying course material for trainings that have been given within the frame of the CIPRNet project (www.ciprnet.eu). The first objective of this document is to provide a general introduction into model coupling. Learning goal is to know basics of different coupling methods and different modes of process interaction modelling. The second section provides technical explanation of the OpenMI standard. Students learn what an OpenMI compliant component is and learn how the data exchange works. The third section accompanies the OpenMI life demonstration, where two OpenMI-compliant models are loaded and connections between models are configured. This document also contains a reference list for further reading.

B. Becker (✉) · A. Burzel
Deltares, P.O. Box 177, 2600 MH Delft, The Netherlands
e-mail: bernhard.becker@deltares.nl

A. Burzel
e-mail: andreas.burzel@deltares.nl

R. Setola et al. (eds.), *Managing the Complexity of Critical Infrastructures*,
Studies in Systems, Decision and Control 90,
DOI 10.1007/978-3-319-51043-9_11

2 Model Coupling and Conjunctive Modelling

2.1 What Is a Model?

> A model should be made as simple as possible, but not simpler.
>
> (after Albert Einstein, 1879–1955)

Following Konikow and Bredehoeft [1] we use the following definitions:

A *model* is a representation of a real system or process. A *conceptual model* is a hypothesis for how a system or process operates. *Mathematical models* are abstractions that replace objects, forces, and events by expressions that contain mathematical variables, parameters and constants. *Deterministic models*, also called physics-based models, are based on the conservation of mass, momentum and energy. Deterministic models often require the solution of differential equations for certain boundary and initial conditions. A mathematical model, or, more in particular, a numerical algorithm to solve differential equations, implemented into computer code is called a *computer model*. This computer model can also be considered as a *generic model*. When model parameters, boundary conditions and grid definitions for a generic model are specified to represent a particular geographic area, we obtain a *site-specific model*, including model data and software. A *synthetic model* represents a fictitious site, often used to illustrate or analyse a certain process.

A computer model usually consists of a graphical user interface part and a computational core that solves the partial differential equation system.

Flow processes are often described mathematically by partial differential equations. These equations cannot be solved analytically. The numerical solution requires a grid (mesh) that represents the modelling area. The solution of differential flow equations requires a full definition of the boundary of the modeling area, the so-called boundary conditions. In addition, internal boundary conditions like sources and sinks can be defined. Transient flow problems require initial conditions for the whole modeling area grid. A set of boundary conditions and initial conditions is called *scenario*.

2.2 What Is Conjunctive Modelling?

Conjunctive modelling means to link site-specific models in such a way that the interaction processes between the domains the models represent are modelled on a time-step basis. There are different levels of conjunctive modelling: model coupling means data transfer in two directions, while an uncoupled approach has data exchange in one direction only.

If models are coupled, the simulation results of the first model have an impact on the second model and vice versa. This means that coupled models must exchange data during runtime on a time step basis. In case of uncoupled conjunctive

modelling the simulation results of the first model have an impact on the second one, but the simulation result of the second model has no feedback impact on the first model.

According to Morita and Yen [2, 3], there are three levels of model coupling:

- simultaneous coupling
- alternating iterative coupling
- externally coupling.

External coupling means data exchange once per time step in both directions. Results from one model are used as boundary conditions in the other one and vice versa (see Fig. 1a). This is the lowest level of model coupling. Also called time-lagged approach [4, 5] this approach is the least accurate one, because it contains inherent mass balance and momentum balance errors. But this approach is certainly the most often applied one, because it is easier to implement than the other two, and often sufficient.

Iterative coupling means to exchange data between models not only once per time step, but to iterate the exchange of data until a certain convergence criterion is achieved (see Fig. 1b). Consequently, mass balance errors and momentum errors are basically smaller than for external coupling. But this method is more difficult to implement and more computational expensive.

Simultaneous coupling is the highest level of model coupling. It means to represent different processes, including the interactions, in one equation system. However, the simultaneous solution requires equal time stepping for all coupled processes, and the equations should be of the same type to make it efficient.

OpenMI supports iterative coupling and external coupling. Morita and Yen [2] and Becker and Talsma [6] discuss numerical aspects of these model coupling approaches.

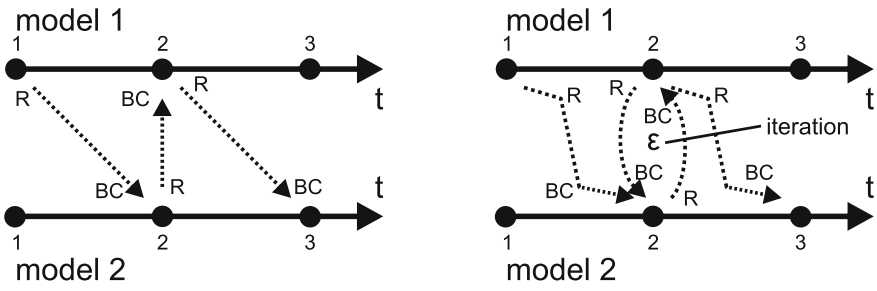


Fig. 1 Functional principle of external coupling and iterative coupling of two models (after Becker [28]). *R* result, *BC* boundary condition, *t* time, ε convergence criterion

As uncoupled approach we consider the successive execution of two model simulations where the first model produces boundary conditions for the second one. A feedback from the second one to the first is not incorporated. An uncoupled conjunctive modelling can be realized by simple exchange of input and output files between models. The easiest way to implement such an uncoupled conjunctive modelling is to implement simulation results from one model as boundary conditions for the second model manually or script-based. OpenMI can help to improve efficiency for uncoupled conjunctive modelling as shown by Becker and Schüttrumpf [7]. More advanced approaches of uncoupled conjunctive modelling incorporate a data integration platform like Deft-FEWS [8].

2.3 Task

Your task is the design of a model chain for the following scenario:

1. Heavy rainfall causes high water in a river.
2. High water in a river causes dike breach due to overtopping.
3. The dike breach causes inundations of the hinterland.
4. From the inundated areas water infiltrates into the subsurface and causes groundwater head rise.
5. Rising groundwater levels create uplift forces on a road tunnel and flows cellars with information technology installation.

Carry out the following working steps:

1. Identify the relevant processes and the corresponding models.
2. Draw a flow chart with the models and their interactions. Indicate the direction of data transfer with arrows.
3. Explain your model chain.
4. Discuss alternative set-ups.

A possible solution of task 1 is given in Table 1. A solution for task 2 is given in Fig. 2. A possible explanation of the model chain (task 3) is

Table 1 Relevant processes and corresponding models

No.	Process	Model
1	Rainfall-runoff	Hydrological model
2	River flow	1D open channel flow model
3	Dike breach	Dike breach model
4	Hinterland flooding	Two-dimensional flood model
5	Groundwater head rise (subsurface flood)	Groundwater model

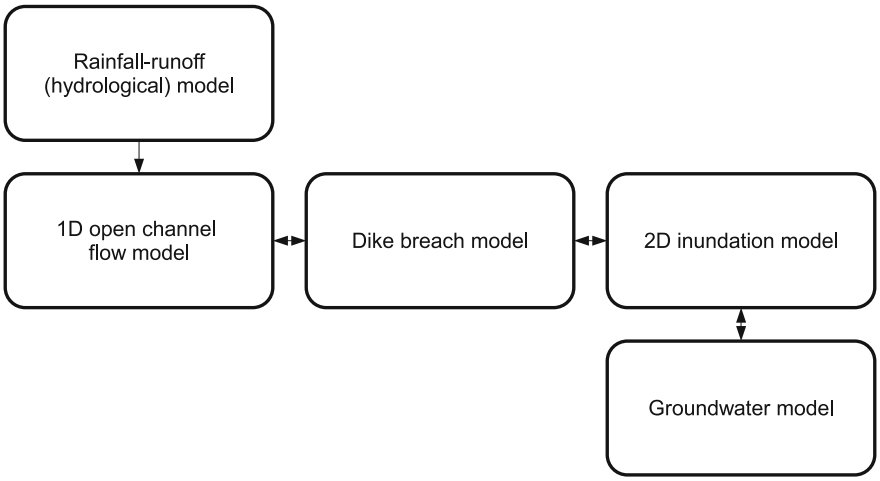


Fig. 2 Model coupling for process interaction modelling. *Arrows* indicate data exchange between models to represent process interaction

- Rainfall runoff feeds the open channel flow, but the open channel flow processes have no impact on the rainfall-runoff. So the data transfer is unidirectional and the interactions can be modeled uncoupled.
- River flow, dike breach and inundation are processes that interact with each other. Uncoupled modelling would violate the mass balance of water, so a coupled approach is chosen.
- The infiltration of water from inundated areas into groundwater is an interaction process which cannot be modelled uncoupled, because infiltrating water affects the inundation area and the groundwater balance.
- The model chain provides information that can be used to identify endangered critical infrastructure. The infrastructure itself has no impact on the hydrological processes, so the simulation results can be transferred to critical infrastructure models manually.

Alternative setups (task 4):

- A connection between the river model and the groundwater model adds the process of bank storage to the system model.
- Interactions between river model, dike breach model and two-dimensional flow model could be made uni-directional to trade-off accuracy against performance.
- A geotechnical model for failure mechanisms due to uplift forces can be added to the modelling chain.

3 The OpenMI Standard

3.1 Introduction

The OpenMI standard defines an interface that allows time dependent models to exchange data at runtime [9]. Model components that comply with the OpenMI standard can, without any programming, be coupled to OpenMI modelling systems [10, 11]. The OpenMI environment provides tools that facilitate the migration of legacy code. This grants a high acceptance of coupled models by users, because they can use their already existing models in coupled simulations. The initiative for OpenMI originates from the water sector, but OpenMI has already reached a wider distribution than the water domain only (see e.g. Bulatewicz et al. [12]).

Beside the standard interface specification, the OpenMI-association [13] also provides the OpenMI environment. This is a software that assists in the implementation of the OpenMI standard. It contains compiled .NET assemblies and the source code of all packages and their documentation [9]. The OpenMI environment also provides the OpenMI configuration editor. This programme supports the data exchange between different OpenMI compliant components.

An OpenMI system is a software system where different OpenMI compliant components are connected to a coupled modelling system. The OpenMI data exchange is based on a pull-driven request-reply mechanism. One component, for example a site-specific model, requests data needed for the own computation from another component. Components can be connected in different manners:

- unidirectional connection
- bidirectional connection
- iterated connection.

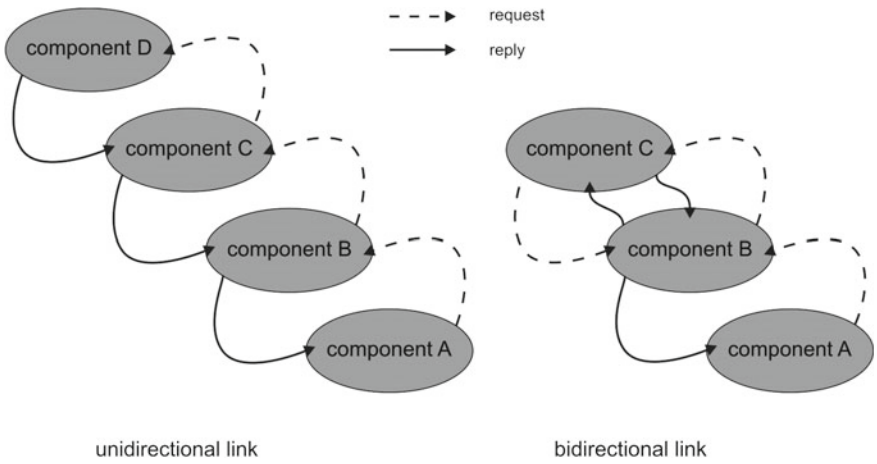


Fig. 3 Different connection layouts with the request-reply mechanism (after Gregersen et al. [10])

According to Sect. 2.2, unidirectional connection supports the uncoupled approach, the bidirectional connection is for external coupling and the iterated connection helps to realize an iterated coupling with OpenMI. The simultaneous solution cannot be achieved with OpenMI.

In Fig. 3, different layouts of pull-driven request-reply connections are shown. For the unidirectional chain, component A requests B for data. In order to response, it needs data from another component itself and requests C for data, which again requests data from component D. D is at the end of the chain and performs its computation first and then answers C. C is now able to compute and answers the request of component B afterwards. B now calculates with the data from C and is able to respond on the request of A. For the bidirectional connection example, component A requests data from B. B needs data from component C. To fulfil this request, C needs data from B. Because B waits for data from C itself, it gives a guess to C. C computes with this guess and can now response to B. B is now able to compute and to reply to the request of A.

Both examples show, that one component must initialize the computation with a request to define which component shall compute first. That is why each OpenMI system contains an element which triggers the simulation. For the bidirectional connection, simulation results may differ depending on which component computes first and gives a guess. Gregersen et al. [10] call this coupling semi-explicit, because the results of one component are based on a guess, but the results of the other component are based on a calculation. The iterative connection is an advanced bidirectional connection. In the example of Fig. 3 (right side), components B and C would adjust their reply values iteratively until an accuracy criterion is fulfilled.

3.2 *OpenMI Composition Components*

The `omi`-file contains information about one single OpenMI compliant component:

Table 2 `omi`-file for a SOBEK model

```
<?xml version="1.0"?>
<LinkableComponent xmlns="http://www.openmi.org"
  Type="DeltaShell.OpenMIWrapper.DeltaShellOpenMILinkableComponent"
    Assembly=".\bin\DeltaShell.OpenMIWrapper.dll">
  <Arguments>
    <Argument Key="DsProjFilePath" ReadOnly="true"
      Value=".\SobekRiverFlowModel\Magdeburg3.dsproj" />
    <Argument Key="ModelName" ReadOnly="true" Value="integrated model" />
    <Argument Key="ResultingDsProjFilePath" ReadOnly="true"
      Value=".\SobekRiverFlowModel\MagdeburgRTC.dsproj" />
    <Argument Key="SplitSpecificElementSets" ReadOnly="true"
      Value="CalcPoints;Laterals;Structures;Measurements" />
  </Arguments>
</LinkableComponent>
```

- Where is the DLL with the computational core and OpenMI-Interface?
- Where is the working directory with input files?
- Anything else like command line arguments or specific settings?

The omi-files are structured in xml. The omi-file must be created by the modeller. An example of an omi-file is given in Table 2.

Table 3 opr-file for an OpenMI composition with a SOBEK model and an RTC-Tools model

```
<guiComposition version="1.0">
  <models>
    <model omi="d:\OpenMIcourse\OpenMICoursePackageElbe\RtcTools.omi"
      rect_x="195" rect_y="113" rect_width="100" rect_height="51" />
    <model omi="d:\OpenMIcourse\OpenMICoursePackageElbe\ElbeSobek.omi"
      rect_x="52" rect_y="112" rect_width="100" rect_height="51" />
    <model omi="Oatc.OpenMI.Gui.Trigger"
      rect_x="196" rect_y="30" rect_width="100" rect_height="51" />
  </models>
  <links>
    <uilink
      model_providing="integrated model"
      model_accepting="RtcTools_ModelId">
      <link id="2"
        source_elementset="ObservationPoint1"
        source_quantity="Water level (op)"
        target_elementset="Water level (op)@ObservationPoint1"
        target_quantity="Water level (op)" />
    </uilink>
    <uilink
      model_providing="RtcTools_ModelId"
      model_accepting="integrated model">
      <link id="4"
        source_elementset="Crest level (s)@Weir1"
        source_quantity="Crest level (s)"
        target_elementset="Weir1"
        target_quantity="Crest level (s)" />
    </uilink>
    <uilink
      model_providing="integrated model"
      model_accepting="Oatc.OpenMI.Gui.Trigger">
      <link id="6"
        source_elementset="Node001"
        source_quantity="water_level"
        target_elementset="TriggerElementID"
        target_quantity="TriggerQuantityID" />
    </uilink>
  </links>
  <runproperties
    listenedeventtypes="11111111111"
    triggerinvoke="01/26/2000 00:00:00"
    runinsamethread="0" showeventsinlistbox="1"
    logfilename="CompositionRun.log" />
  <mainForm width="360" height="277" />
  <sdk>
    <smartbuffer maxnumberoftimes="0" />
  </sdk>
</guiComposition>
```

3.3 Connections

The opr-file defines how OpenMI components are connected within an OpenMI composition and contains runtime information:

- Which components are part of the composition (reference to omi-files and trigger component)?
- Which connections are defined between components?
- Details of the connections (what and where)?
- Simulation period.

The opr-file is created by the OpenMI configuration editor, but can be modified by the modeller. Like the omi-file, the opr-file is structured in xml. Table 3 gives an example for an opr-file.

A connection between model components consists of links. A link is defined between an output exchange item and an input exchange item of two different model components, respectively. An exchange item defines a simulation time related quantity and its unit for an ordered set of elements, e.g. a single node number, a node coordinate, or lines, polygons or polyhedrons. Input exchange items usually form boundary conditions in an OpenMI compliant model component, while output exchange items are mostly simulation results.

During simulation, the exchange item is assigned with a value. This gives the OpenMI compliant component the following information:

- the *value* itself,
- *what* the value represents (quantity and unit),
- *where* the value applies (element set),
- and *when* the value applies.

The OpenMI compliant component is responsible to provide the data in a correct way and for what to do with received data.

3.4 Making (Legacy) Code OpenMI Compliant

An OpenMI-compliant model satisfies the following criteria:

1. The model must be able to submit to run-time control by an outside entity.
2. The model must be structured in such a way that initialization is separate from computation.
3. The model must be able to expose information on the modelled quantities it can provide.
4. The model must be able to provide the values of the modelled quantities for any requested point in time and space.

5. The model must be able to respond to a request; if the response requires data from another component, the model must be able to pass on the time in its own request.
6. A delivering model component must know what time it has reached. It must recognize whether it has not yet reached the requested time, it is at the requested time or it has passed the requested time.
7. Components must be able to interpolate if the requested time is not in their own time step or space frame.
8. Components must know when they are waiting for data, and in which case they will have to return an extrapolated value.

Since OpenMI is an interface standard, the implementation of the interface requires modifications of the source code of a mode component that shall run within OpenMI compositions. The easiest way to make a generic model OpenMI-compliant is to embed the code into a wrapper class provided by the OpenMI environment [14]. Therefore, the code usually has to be reorganized. The wrapper controls the run-time activity of pulling data across links. The OpenMI environment provides a "smart wrapper" that already handles most of the tedious and difficult tasks to be performed, for example items 3–8 from the list above.

An OpenMI compliant model component is loaded into the OpenMI configuration editor as dynamic link library (DLL). To comply with the OpenMI standard, a component must provide several functions (OpenMI methods). Examples for those methods concerning the structure of the programme are listed below [14]:

1. `Initialize()`
2. `PerformTimeStep()`
3. `Finish()`
4. `Dispose()`

The method `Initialize` usually comprises the opening and reading of input files describing the mesh, initial conditions and boundary conditions. `PerformTimeStep` initializes the computation of one time step. The `Finish` method has been prepared to close all files used by the component; within the `Dispose` method, allocated memory is freed. The most important OpenMI methods for the data exchange itself are given in the following list:

- `GetCurrentTime()`
- `GetValues(QuantityID, ElementSetID)`
- `SetValues(QuantityID, ElementSetID, values)`

`GetCurrentTime` returns the point in time a component has reached. `GetValues` returns values related to output exchange items (simulation results) for the current time. The function arguments indicate what the return value represents and where it is located. The `SetValues` method sets a value for the model component as an answer on a request. The value to set is a function argument and is usually used as a boundary condition value by the model.

3.5 Example Cases of Conjunctive Modelling with OpenMI

Example cases of conjunctive modelling with OpenMI under contribution of the authors of this document are given in the following list:

- Generation of boundary conditions for a transient dam seepage scenario [7].
- Modelling of surface-subsurface interactions, i.e. bank storage and vertical infiltration from a flooded area [15].
- Coupling of an open channel flow model with a pump model to design a large pump station [16].
- Coupling of models of the same type: two open channel flow models are coupled to bridge administrative boundaries [17, 18].
- Integration of different hydrological processes [19].
- Real-time control of hydraulic structures in open channel flow models to model the human interactions in a water system [20–23].

See also the OpenMI website www.openmi.org for more publications.

4 Example: Coupled Flow Simulation and Control

4.1 Study Area and Modelling Objective

The study area is a part of the Elbe river at Magdeburg (Germany). An overview of the study area is given in Fig. 4. The modelling objective is to manage the river in such a way that the water levels remain below the flood warning level. Beside the city of Magdeburg, the critical infrastructure

- main station and
- two railway junctions

might be affected in case of flooding.

4.2 Approach

The relevant processes are

- open channel flow in the section of the river Elbe and
- human operations in the river system (control of hydraulic structures).

We use two models to represent these processes:

- a SOBEK open channel flow model for the flow of water in the Elbe river and
- a real-time control model RTC-Tools to represent the human operations in the water system.

Fig. 4 Study area (taken from www.maps.google.com)

4.3 The SOBEK Open Channel Flow Model

The SOBEK open channel flow model is a deterministic model that simulates water flow in rivers by solving the Saint-Vanant equations with the so-called staggered grid numerical scheme [24].

The SOBEK schematization "Elbe at Magdeburg" is shown in Fig. 5. The water system model network has the following characteristics:

- one branch in the south
- one branch in the north
- two branches in the centre, one representing the main river and one represents the Old Elbe branch

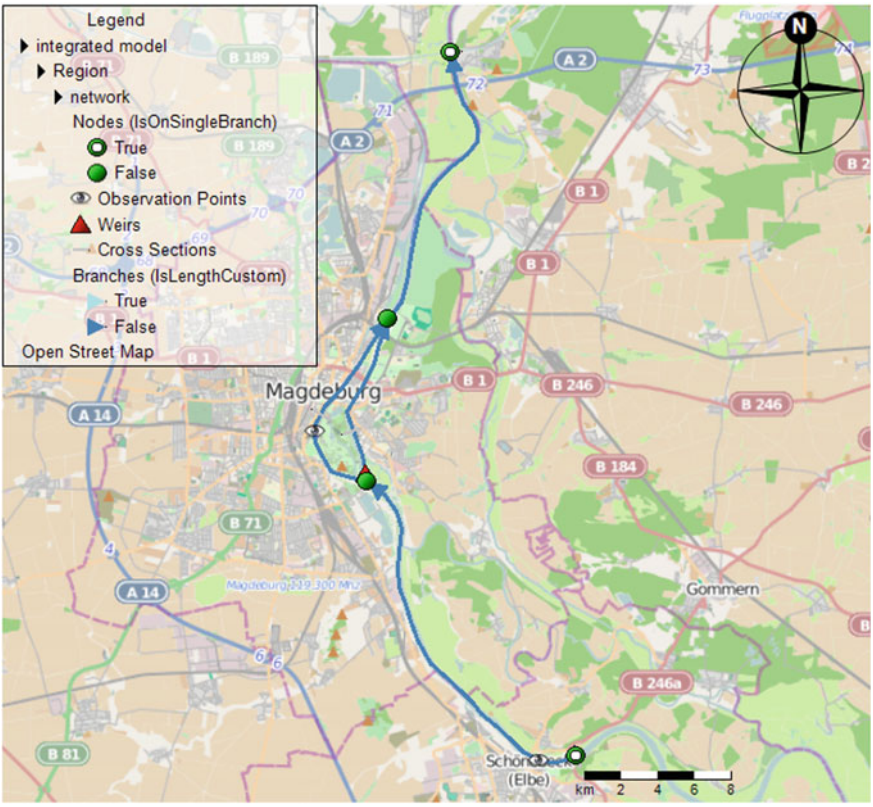


Fig. 5 SOBEK open channel flow model network. Water flows from south to north (background map from www.openstreetmap.org)

- cross sections
- observation points
- one weir to close the Old Elbe branch on its upstream end.

The upstream boundary condition is a discharge time series, as downstream boundary condition a rating curve (discharge-water level relation) is set.

Task:

- Open the SOBEK model.
- Inspect the network: find the observation points and the structure.
- Look at the inflow boundary.
- Run the model.
- Inspect the side-view for the two routes “Elbe” and “Old Elbe”.
- Look at the hydrographs for the two observation points.

For modelling with SOBEK see the user manual [25].

4.4 The RTC-Tools Real-Time Control Model

The RTC-Tools model [22, 26] addresses the control of the weir which is represented in the SOBEK model as structure node. The control is based on water level observations at the Schönebeck gauge in the upstream part of the model. The gauge is represented in the SOBEK model as observation point. The control flow is given in Fig. 6 as a decision tree. This RTC-Tools model is not a deterministic model, but belongs to the group of logical models.

A trigger evaluates if the observed water level at Schönebeck is greater than 54 m. If the condition is true, the weir is opened, if not, the weir is closed. This simple operational protocol ensures sufficient water depth for cargo ship navigation in the main channel of the Elbe during normal condition and reduces the water level during high water conditions.

Task:

- Open the file `rtcToolsConfig.xml`.
- Find the trigger and rule elements from the flow chart in Fig. 6.

See the manual [27] for details on working with RTC-Tools.

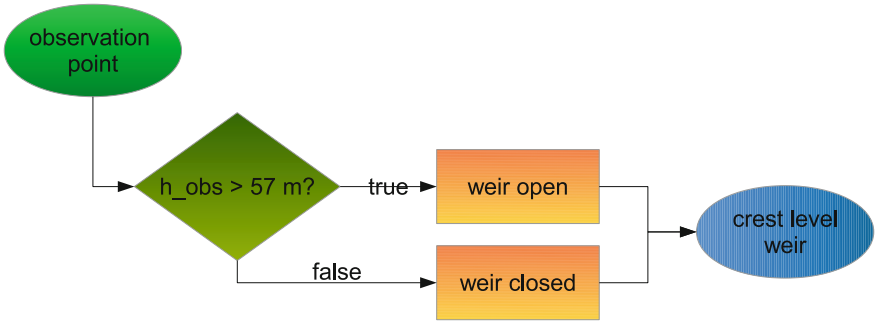


Fig. 6 Flow chart for the control of the weir as modelled with RTC-Tools

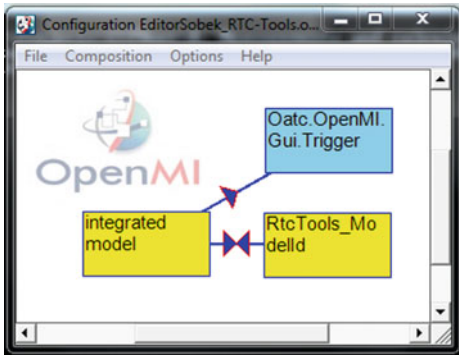


Fig. 7 OpenMI Configuration Editor with a SOBEK model component, an RTC-Tools model component and an OpenMI trigger component

4.5 Coupling with OpenMI

The interaction of human control and open channel flow is as follows:

- the crest level of the weir is controlled in dependence of the current water level at the observation point and
- the control of the weir has an impact on the water system:
  - if the weir is open, water can flow through the main branch and the Old Elbe branch
  - if the weir is closed, the water flows through the main Elbe branch only.

To model this interaction, bi-directional data exchange has to be configured as follows:

- SOBEK provides the water level at Schönebeck gauge to RTC-Tools
- RTC-Tools provides the crest level for the weir to SOBEK.

Task:

- Open the OpenMI configuration editor.
- Load the RTC-Tools model into the OpenMI configuration editor.
- Load the SOBEK model into the OpenMI configuration editor.
- Add a trigger component to the composition. Note that the OpenMI trigger should not be confused with the RTC-Tools trigger element.
- Add a connection from the RTC-Tools model to the SOBEK model and configure the connection as shown in Fig. 8.
- Add a connection from the SOBEK model to the RTC-Tools model and configure the connection as shown in Fig. 9.

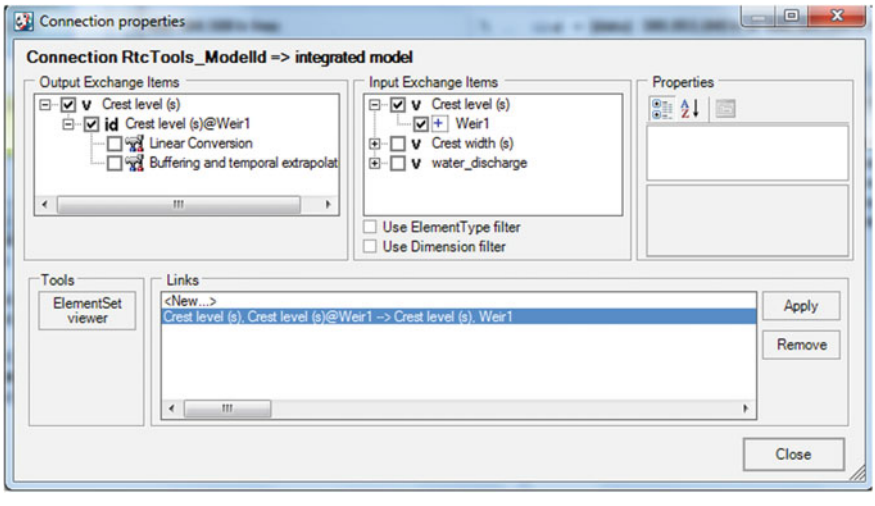


Fig. 8 Connection properties RTC-Tools—SOBEK

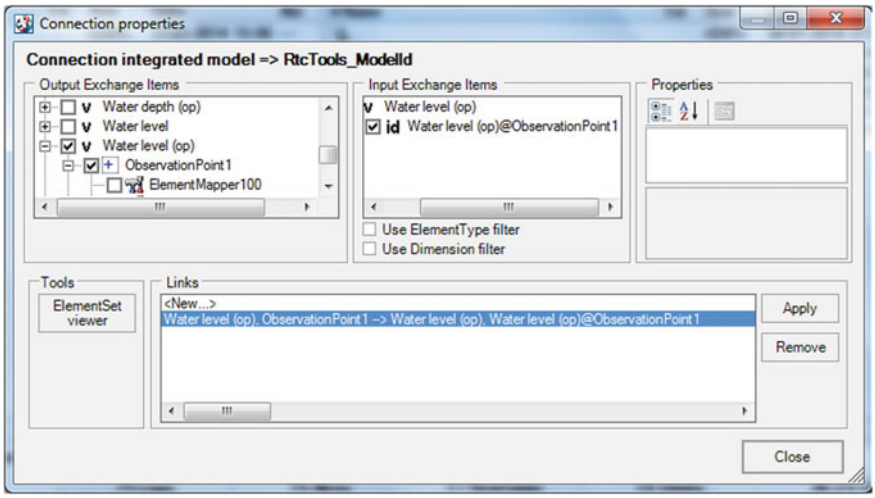


Fig. 9 Connection properties SOBEK—RTC-Tools

- Add a connection from the SOBEK model to the OpenMI trigger and configure the connection as shown in Fig. 10. Choose an arbitrary exchange item from the SOBEK model.
- Save the composition. The OpenMI composition should look like the one in Fig. 7.

The functional principle of the data exchange is shown in Fig. 11. The data exchange procedure can be summarized as follows [6]:

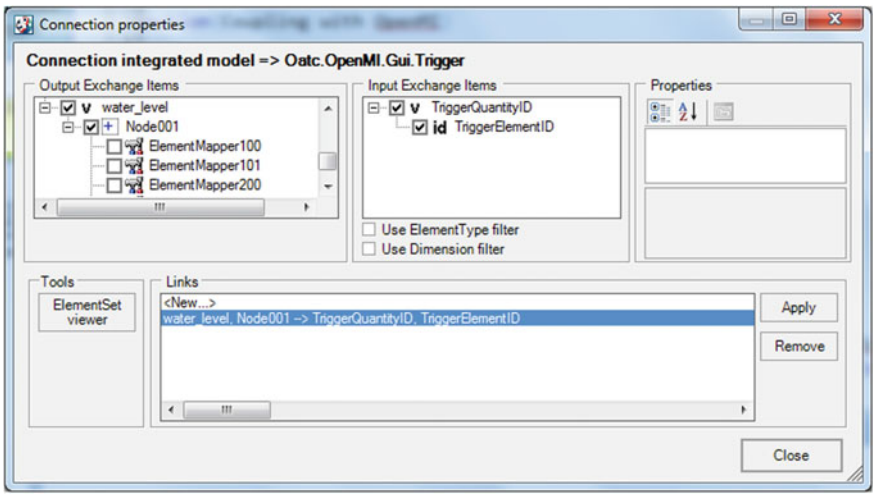


Fig. 10 Connection properties SOBEK—OpenMI trigger

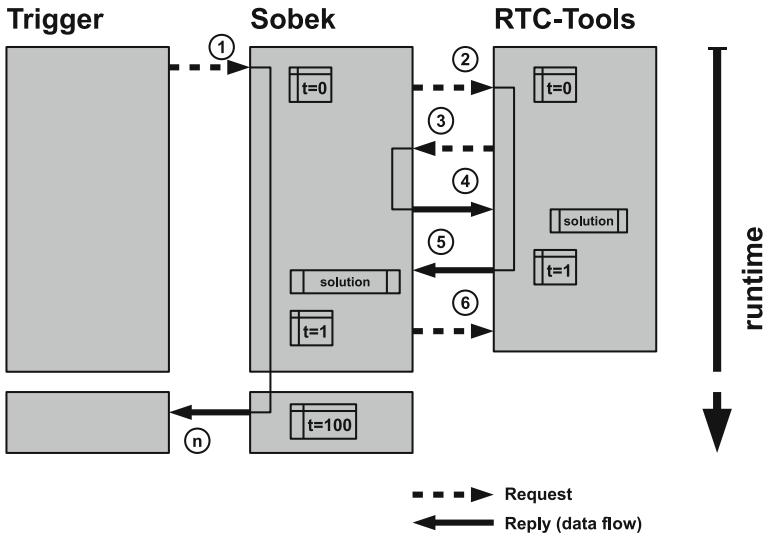


Fig. 11 Request-reply mechanism for an OpenMI composition with SOBEK and RTC-Tools

- The model component that asks first computes last.
- The model that asks gives the guess (i.e. data from the previous time step).

The OpenMI trigger element has been connected to the model component in such a way that RTC-Tools is the first model that computes the solution for a given time step. In order to compute the control action for the current time step, RTC-Tools uses observed data from SOBEK from the previous time step. This time lag (see also Sect. 2.2) is usually a source of inaccuracy when coupling physical processes, but in the current case it ensures that a control action takes effect in the water system *after* the observation that triggers the control action has been made.

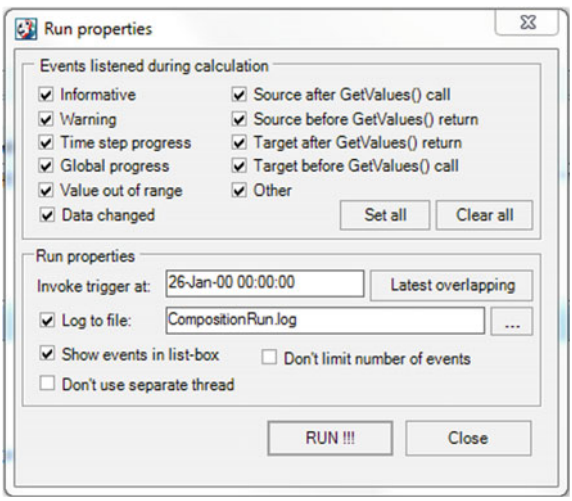


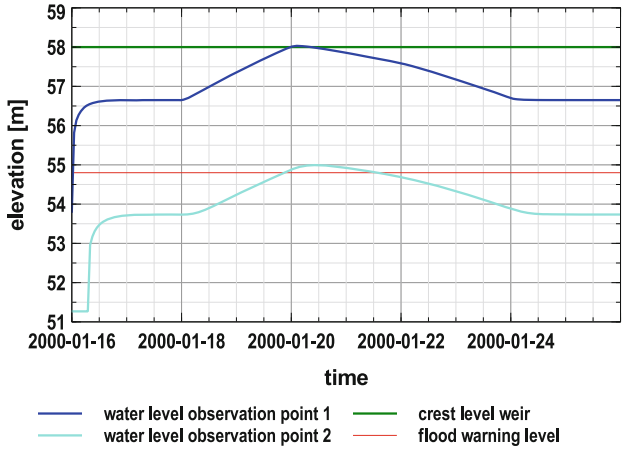
Fig. 12 OpenMI configuration editor Run properties window

4.6 Coupled Simulation and Simulation Results

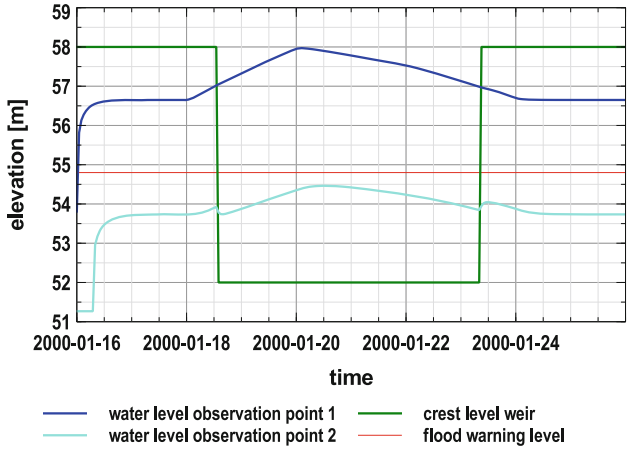
Task:

- Run the OpenMI composition via the Run properties window (Fig. 12).
- Open the SOBEK model that has been running within the OpenMI coupled simulation.
- Inspect the side views for the routes “Elbe” and “Old Elbe”. For the latter one, add the coverage “Crest level(s)”.
- Inspect the hydrographs of the two observation points and the crest level.

Figure 13 shows simulation results from the SOBEK model with an uncontrolled weir (Fig. 13a) and the simulation results from the coupled simulation



(a) Simulation results from the SOBEK model (channel flow)



(b) Simulation results from the coupled flow simulation with SOBEK (channel flow) and RTC-Tools (control)

Fig. 13 Simulation results

SOBEK—RTC-Tools (Fig. 13b), where the weir is controlled in dependence of the water level at Schönebeck gauge (observation point 1). In the coupled simulation the water level at the observation point "Magdeburg" (observation point 2) remains below the flood warning level of 54.8, because the weir has been opened after the water level at Schönebeck gauge has reached 57. At the bifurcation point the water divided into the Old Elbe branch which results in a lower water level in the main branch of the Elbe.

Acknowledgement and Disclaimer This chapter was derived from the FP7 project CIPRNet, which has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 312450.

The contents of this chapter do not necessarily reflect the official opinion of the European Union. Responsibility for the information and views expressed herein lies entirely with the author(s).

References

1. Konikow LF, Bredehoeft JD (1992) Ground-water models cannot be validated. Adv Water Resour 15:75–83
2. Morita M, Yen BC (2000) Numerical methods for conjunctive two-dimensional surface and three-dimensional sub-surface flows. Int J Numer Meth Fluids 32:921–957
3. Morita M, Yen B (2002) Modeling of conjunctive two-dimensional surface-three-dimensional subsurface flows. J Hydraul Eng 128(2):184–200. doi:10.1061/(ASCE)0733-9429(2002)128:2(184)
4. Fairbanks J, Panday S, Huyakorn PS (2001) Comparisons of linked and fully coupled approaches to simulating conjunctive surface/subsurface flow and their interactions. In: MODFLOW 2001 and other modeling odysseys—conference proceedings, Golden, CO, p 356–361
5. Huang G, Yeh GT (2006) An integrated media, integrated processes watershed model—wash123d: part 3—a comparative study on different surface water/groundwater coupling approaches. In: Binning PJ, Engesgaard PK, Dahle HK, Pinder GF, Gray WG (eds) Proceedings of the XVI international conference on computational methods in water resources, Copenhagen, Denmark.
6. Becker B, Talsma J (2013) On the external and iterative coupling of multiple open channel flow models with OpenMI. Rev Ing Innova 6:55–66
7. Becker BPJ, Schüttrumpf H (2010) An OpenMI module for the groundwater flow simulation programme Feflow. J Hydroinform 13(1):1–13. doi:10.2166/hydro.2010.039. URL http://www.iwaponline.com/jh/013/jh0130001.htm
8. Werner M, Schellekens J, Gijsbers P, van Dijk M, van den Akker O, Heynert K (2013) The delft-FEWS flow forecasting system. Environ Model Softw 40:65–77. doi:10.1016/j.envsoft.2012.07.010. URL http://linkinghub.elsevier.com/retrieve/pii/S1364815212002083
9. Moore R, Gijsbers P, Fortune D, Gregersen J, Blind M (2005) OpenMI document series: part A—scope for the OpenMI, version 1.0 edn. URL http://www.openmi.org/openminew/documents/A_OpenMI_Scope.pdf
10. Gregersen J, Gijsbers P, Westen S (2007) OpenMI: Open modelling interface. J Hydroinformatics 9(3):175–191. doi:10.2166/hydro.2007.023
11. Moore RV, Tindall CI (2005) An overview of the open modelling interface and environment (the OpenMI). Environ Sci Policy 8(3):279–286. doi:10.1016/j.envsci.2005.03.009

12. Bulatewicz T, Yang X, Peterson JM, Staggenborg S, Welch SM, Steward DR (2010) Accessible integration of agriculture, groundwater, and economic models using the open modeling interface (OpenMI): methodology and initial results. Hydrol Earth Syst Sci 14 (3):521–534. doi:10.5194/hess-14-521-2010. URL http://www.hydrol-earth-syst-sci.net/14/521/2010/
13. OpenMI Association (2014) OpenMI. URL http://www.openmi.org
14. Gijsbers P, Gregersen J, Westen S, Dirksen F, Gavardinas C, Blind M (2005) OpenMI document series: Part B—Guidelines for the OpenMI. IT Frameworks (HarmonIT), version 1.0 edn. URL http://www.openmi.org/openminew/documents/B_Guidelines.pdf
15. Becker BPJ, Forberig S, Flögel R, Schüttrumpf H, Köngeter J (2011) On the determination of groundwater levels for hazard maps of groundwater head rise induced by high water. Wasserwirtschaft 12:10–16 (in German)
16. Becker B, Dahm R, van Heeringen KJ, Goorden N, Kramer N, Kooij K, Gooijer J, Jansen J (2012a) Op zoek naar een optimaal ontwerp voor een groot uitwateringsgemaal in het Lauwersmeer. H_2O 44(13):11–13 (in Dutch)
17. Becker B, Gao Q (2012) Koppelen Sobek-modellen "Wetterskip Fryslân" en "Waterschap Noorderzijlvest" via OpenMI. Report 1204514-000-ZWS-0007, Deltares, Delft (in Dutch)
18. Becker BPJ, Talsma J, Gao Q, Ruijgh E (2012c) Coupling of multiple channel flow models with OpenMI. In: Proceedings of 10th international conference on hydroinformatics, Hamburg, Germany
19. Schellekens J, Becker BPJ, Donchyts G, Goorden N, Hoogewoud JC, Patzke S, Schwanenberg D (2012) OpenStreams: open source components as building blocks for integrated hydrological models. In: Geophysical research abstracts, Vienna, Austria, vol 14 EGU2012, p 3953. URL http://adsabs.harvard.edu/abs/2012EGUGA..14.3953S
20. Becker BPJ, Schwanenberg D, Schruff T, Hatz M (2012b) Conjunctive real-time control and hydrodynamic modelling in application to Rhine River. In: Proceedings of 10th international conference on hydroinformatics, TuTech Verlag TuTech Innovation GmbH, Hamburg, Germany
21. Becker B, Schruff T, Schwanenberg D (2014) Modellierung von reaktiver Steuerung und Model Predictive Control (Modelling of reactive control and model predictive control). In: Selbstverlag der Technischen Universität Dresden (Simulation techniques and models for hydraulic engineering and water management), Dresden, Wasserbauliche Mitteilungen, vol 50, p 165–174 (in German)
22. Schwanenberg D, Becker BPJ, Xu M (2015) The open RTC-Tools software framework for modeling real-time control in water resources systems. J Hydroinform 17(1):130–148. doi:10.2166/hydro.2014.046
23. Becker B (2013) Inzet RTC-Tools voor het boezemmodel "wetterskip fryslân". Report 1205773-000, Deltares, Delft (in Dutch)
24. Stelling GS, Duinmeijer SPA (2003) A staggered conservative scheme for every froude number in rapidly varied shallow water flows. Int J Numer Methods Fluids 43:1329–1354
25. Deltares (2014) SOBEK 3/ D-Flow 1D and D-Real time control in delta shell/User manual. Deltares, Delft, version: 3.2.1.31793

26. Deltares (2013) RTC-Tools a toolbox for real-time control of hydraulic structures. URL http://oss.deltares.nl/web/rtc-tools, published: Deltares
27. Deltares (2012) RTC-Tools a software package for modelling real-time control/Technical reference manual and configuration guidelines. Deltares, Delft, version: 0.1.0.22313
28. Becker BPJ (2010) Zur gekoppelten numerischen Modellierung von unterirdischem Hochwasser. Dissertation, RWTH Aachen, Fakutlät für Bauingenieurwesen, Aachen. URL http://d-nb.info/100850209X/34 (in German)