European Technology Platform on
Industrial Safety
Safety for Sustainable European Industry Growth

PLATAFORMA TECNOLÓGICA ESPAÑOLA DE SEGURIDAD INDUSTRIAL

ETPIS-PESI (cross ETP initiative on Industrial Safety and Security towards Resilient Organizations, Infrastructures and Communities)

(Production plants, Utility and Transport networks and critical services for the Smart City)

Integrated approach for Risk Management and Cybersecurity in Critical Infrastructures under Industry 4.0/5.0 towards Resilience

JNIC (Bilbao, 29 June 2022)

Javier LARRAÑETA
PESI Secretario General
ETPIS Executive Board

tecnalia Inspiring Business

tecnal:a
MEMBER OF BASQUE RESEARCH & TECHNOLOGY ALLIANCE

JNIC 2022

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

VII Jornadas Nacionales de
Investigación en Ciberseguridad

Index

- **Context: Critical Infrastructures and industrial accidents (lack of Resilience, dependencies and domino effects)**

- **ETPIS PESI:** European & Spanish Technology Platforms (since 2002/2005) on **integral Industrial Safety & Security**
  - Integral Vision, Governance and Risk Mgt. for the Resilience (Industry, Networks & Infrastructures)
  - Safe & Secure Cities (under CIP: protection of Industrial & Transport Critical Infrastructures)
- **Industrial Safety in ETPIS 2 (SafeFuture for H2030)**
  - Safe-Infrastructures and Resilience

- **Deployment areas: Industrial Safety, OSH, Reliable Operation, Natural Disasters/Climate Change affection, Security and Cybersecurity**

- **Security, Resilience and Critical Infrastructures Protection (Secure Communitties)**
  - Technological priorities in Industry, Networks and relevant Infrastructures

Context: recent dramatic accidents in Critical Infrastructures due to the lack of Resilience (and domino effects)

Industrial accidents: new risks and cascading effects

Industrial and Business activity, Critical infrastructures included, suffer a variety of incidents due to usual operative risks, but a few becomes really grave accidents due to a malevolous combination of risks and non-expected situations

- **Fukushima: nuclear accident** caused originally from a natural disaster (underwater earthquake and tsunami, Japan Sea, 11 March 2011)
- **Blast and fire** in a chemical industry IQOXE (Spain Tarragona, 14 January 2020): two workers died inside the plant and a third citizen at home 3Kms far from the plant (hit by a 1 Tn. reactor part that flighted towards village outside the industrial zone).
- **Ciberatack** (***WannaCry virus***): general affection 3 days to HQs of main Corporations and Critical Infrastructures Operators in Europe (energy, telecomunicationcs…)
- **COVID-19 pandemics (world health crisis, 2020)**: general affection to business activity, Corporations, CI and esential services Operators (value chains)
- **OTHERS**: Ship collapsing Suez Canal (world Logistics); War (Rusia invades Ukraine (European Energy crisis…)




Fukushima: nuclear accident (cascading effects)

El tsunami tras el terremoto afecta gravemente a la infraestructura de protección de la instalación y equipamientos (lo que causó la pérdida del suministro eléctrico a la central, y un grave problema de falta de refrigeración del núcleo.
Todos los reactores operativos en las centrales pararon de forma segura, pero los núcleos de los reactores de dos de las unidades se sobrecalentaron, el combustible nuclear se fundió y las tres vasijas de contención se fracturaron. Las explosiones en los edificios de los reactores causaron daños a estructuras y equipo, así como graves lesiones al personal. Posterior contaminación afectando al medioambiente, poblaciones y sus ciudadanos.

El accidente nuclear de Fukushima (11 de marzo 2011) es un fatal ejemplo de las consecuencias de un conjunto de efectos en cascada:

- Desastre natural
- Afección a la instalación industrial (fallos de fiabilidad y en sistemas de seguridad)
- Accidente industrial grave
- Pérdidas humanas y materiales
- Afección al Medio Ambiente
- Afección a otras Infraestructuras
- Afección reputacional

Fukushima: nuclear accident or the perfect example of dependencies and cascading effects ?

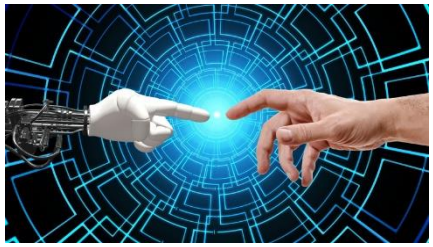
#	Accident steps / Effects	Critical element	Dependency (Intra/Inter)
1	Hearthquake and tsunami (Nature& Climate)	Location of CI	Interdep.
2	Wave destroy coastal infrastructures	Transport infra Energy grid	Interdep.
3	Wave overpass the protection walls of Nuclear plant	Walls (exter-nal perimet)	Intra
4	Water affects electrical appliances (techical failure)	Critical facilities	Intra
5	Cooling system does not work properly (industrial accident)	Critical process	Intra
6	Emergency Team can not avoid the accident nor 1st Responders Access to installations	Team (O&M, external Emergencies)	Intra
7	Control Room cannot stop reactors (heating): Nuclear accident	Critical process	Intra

Industrial Resilience: many key factors to be evaluated

- **Natural disastres** (higher frecuency/intensity, climate change) with severe effects against infrastructures (industry, urban, transport…) and essential serv.
- Other **threats** (**ciberatacks**, terrorist atack, sabotage, technical failures, human errors, lack of maintenance, etc.) and their combination could also produce a series of cascading effects and dramatic consequences.
- Lack of a detailed **dependencies assesment** in the instalations, especially in CI, from others Critical Infrastructures (IC: energy, gas, water, transport network, telecommunications,…);
- Lack of fast alert/**early warning systems** **and** **communication**; insuficient **coordination** **between CI Operators** (and with Public Bodies: **CERTS…**)
- NEW RISKS: **PANDEMICS** (covid19, Humans, Animal & Nature)
- Lack of efficient **protocols** (trans-national/national/regional level) to a fast and effective response to combined emergencies (industrial, disasters natural/social, ciberattack…); although Emergency Plans and Exercises are regularly updated.
- Lack of global integrated **Business Continuity Plans** (on essential service, not only IS) apart from Tecnology Contingency plans and Crisis Mgt.
- And most important: **HUMAN FACTOR** in Security (Cibersecurity) & Resilience

New Societal Challenges and Goals (EU, World)

- Climate Change
- Energy and Mobility
- Natural Resources & Sustainability
- Equity at Society
- Digital Transformation



ETPIS & PESI: Technology Platforms on (integral) Industrial Safety & Security (towards Resilient Infrastructures)

ETPIS - PESI 2020 Vision





« Innovation and technology development (R&D+i) based on a global and integrated vision on Industrial Safety and Risk management»

(Safety + Security)

Four (4) deployment areas:

- **Safety (processes, instalations)**
- **Occupational Safety & Health (Human f.)**
- **Environmental Safety (SHE)**
  (+climate change influence on infrastructures)
- **Corporate Security and Resilience**
  based on the CIP/Cybersec European Directives
  (plants, transport infrastructures & utility networks)

PESI Resilience Ecosystem

1.- Industry (Corps, CI Op., SME and Associations)

- △ Enterprises and Industrial Corporations (many sectors, CIs)
- △ Technology-based SME, Engineering & Consultancy firms)
- △ Associations (Manufacturing, Energy, Security, PPE, Fire, etc)

2.- Government: Ministeries & Regional Bodies

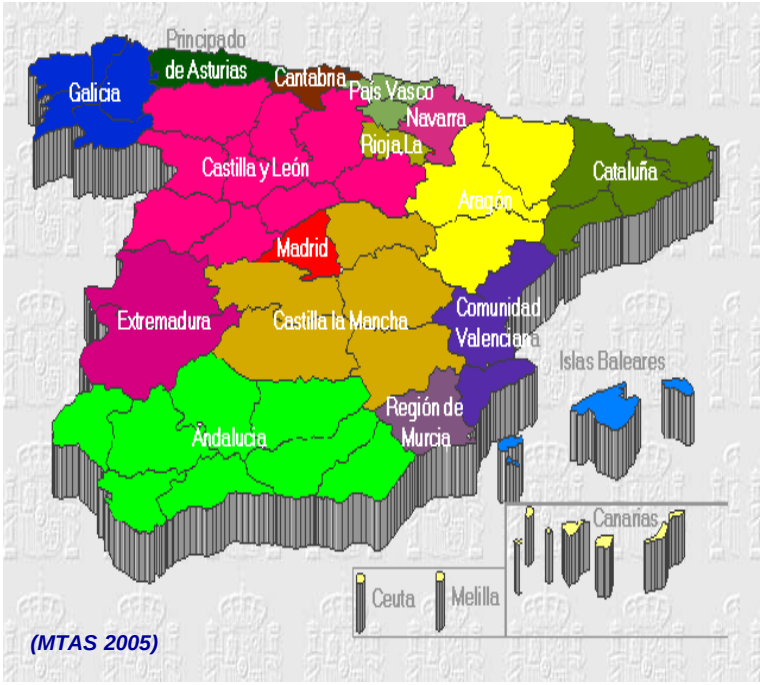
- △ Ministry of Science, and Innovation: AEI, CDTI
- △ Ministry of Industry: Industrial Safety, Connected Industry 4.0
- △ Ministry of Interior (DG PCyE, CNPIC, DG-Traffic)
- △ Min. Economy: Digital Development (INCIBE Cybersecurity)
- △ Ministry of Employment (OSH): INSST
- △ Ministry of Transport and Mobility (Transp. Inf, Haz.Goods…)
- △ Ministry of Ecological Transition: Environment
- △ Public Bodies in Autonomous/Regional Governments

3.- Academia and Research Institutions & Labs

- △ Research Institutes, Labs, Technology Centres
- △ R&D Units at Universities

4.- Other relevant institutions

- △ Normalization and Certification Agents (AENOR)
- △ Insurance companies, Prevention & Health services



2007: 80 Founding Members (non-profit Industry Association)

Around 850 active Organizations +2500 technicians members

European Technology Platform on
Industrial Safety
Safety for Sustainable European Industry Growth

PLATAFORMA TECNOLÓGICA ESPAÑOLA DE SEGURIDAD INDUSTRIAL

SafeFuture

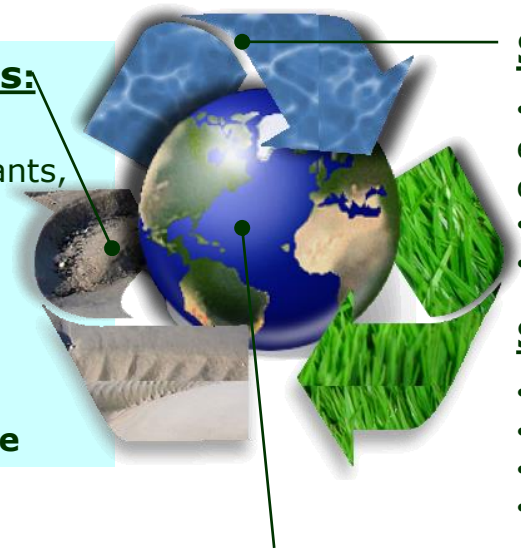
Safety as a trade-mark of the technology "made in EU"

Safe innovation for sustainable future

Way to achieving (by 2020) a new safety paradigm for European industry. Safety as a key factor for successful business and an inherent element of business performance. Industrial safety performance progressively and measurably improved in terms of reduction of reportable accidents at work, occupational diseases, environmental incidents and accident-related production losses. "Incident elimination" and "learning from failures" cultures embedded in design, maintenance, operation at all levels in enterprises. Structured self-regulated safety programs in all major industry sectors in all European countries. Measurable performance targets for accident elimination and accident free mind set workplaces as the norm in Europe.

Safe Infrastructures:

- Safe Life extension of process plants, power plants, transport & utility infra-structure networks, …
- Intensification of NatCat (NaTech)
- Design and monitoring for long term operation
- **Reliability & Resilience**



Safe Energy:

- New safety challenges in renewable energies (wind, H2, solar, bio-fuels, fuel cells, photovoltaic,…)
- Safe energy production and storage
- Smart grids

Safe Products/Production :

- Green jobs
- Value chain and interdependencies
- Nanosafety
- PPEs & Smart Working Environments

Resilience: Protection and Cyber-security

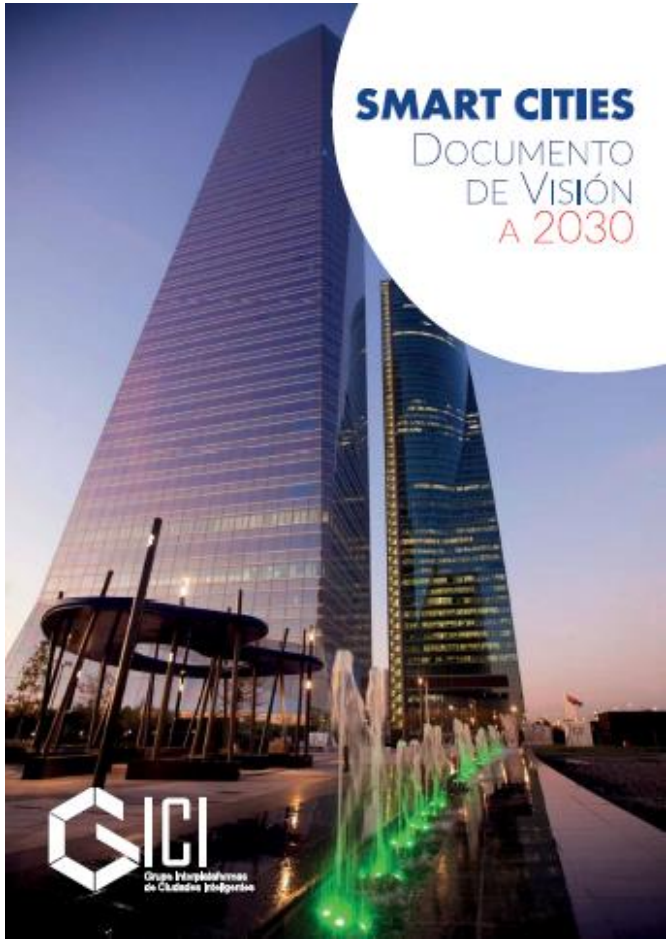
Example: Multi-Risk / Risk-Risk tradeoffs – safety for sustainable integration, interaction and risk governance:

- "Agreed Approach to Risk-Risk Tradeoff management" (the Multi-Risk initiative); difficulties in putting together different risk mitigation policies and ensuring their compatibility

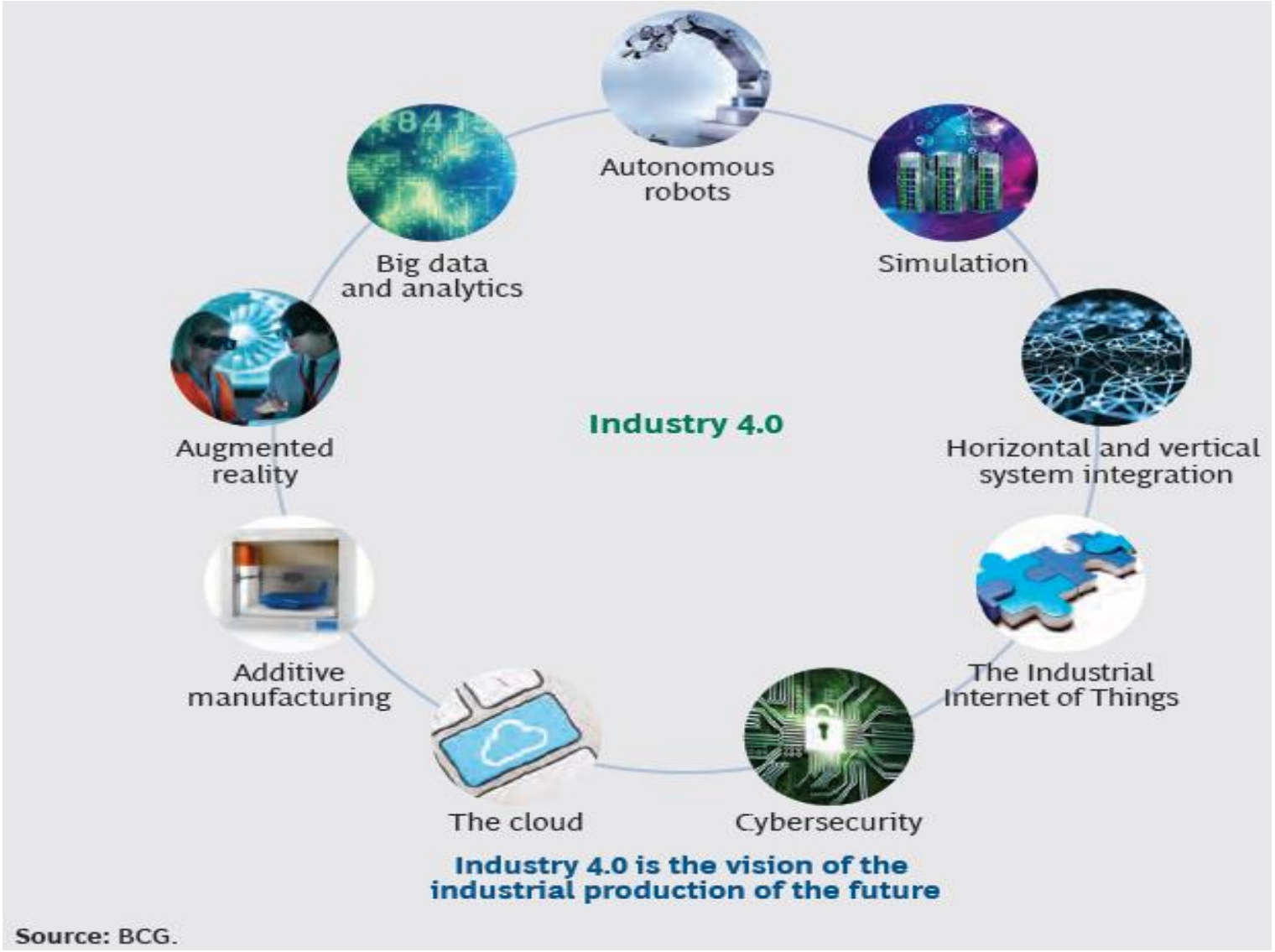
PESI 2030 vision on the Smart & Resilient City

Concept of Secure Society could be very broad from different perspectives *(safety, security, cybersecurity) or* focus (resilience, protection, emergencies, reliability, industrial, road safety, Health, wellbeing…). ETPIS and PESI have fase future challenges for the Smart and Secure Safety & Communities through four **main pillar**:

1. A **Governance model for integral risk management and resilience** of the essential services (CI Operators) for citizens,
2. **Reliability** of Utility networks and urban infrastructures and installations,
3. **Security and protection of citizens, Infrastructures and heritage of the City**
4. And the **cyber-security of control systems in the City** (utilities networks, urban systems and infraestructures related to essential services).



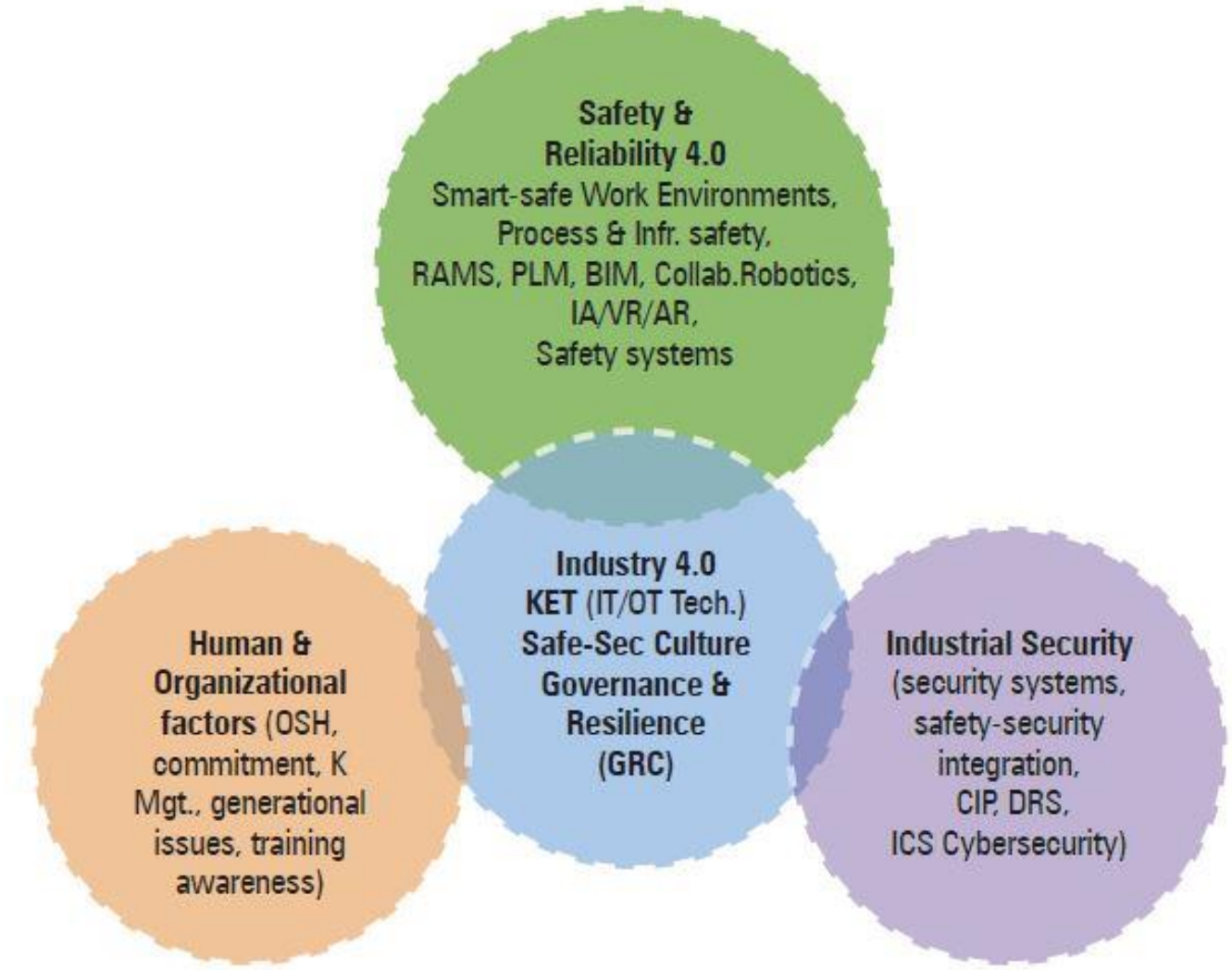
KET Key Enabling Technologies (Industry 4.0/5.0)



Industry 4.0 characteristics

European Commission (2021): focus on People -> I5.0

PESI-ETPIS: Innovation circles for EU Horizon Europe



Industry 5.0 (European Commission)

European Commission

Industry 5.0 and Industrial Safety-Security requirements

INDUSTRY 5.0	TECHNOLOGIES AND INDUSTRIAL SAFETY
CONNECTED	IoT, Cloud, BigData: Process information Integration **Cooperation** Systems/**Workers**, **Internet of All (**Things/Assets/Workers)
AUTOMATED	**Safier &Cybersecure** processes, Early warning Security Systems, Robots (plant, RPAS-Drones…)
FLEXIBLE	Additive manufacturing (3D printing) **Reliability** (RAMS), **Safety** and **Cybersecure** by design
SMART	CPS (Cyber Physical Systems), Artificial Intelligence **Smart PPE, Safety & Protection Systems in S2WE**
SOCIAL	**Human-centered design (OSH)** New (**Safety & Security-Cybersecurity**) Services for Industry and Society. **Resilience** of CI and Essential Services
SUSTAINABLE	Environment-friendly, **Reduction** of Technological **accidents**

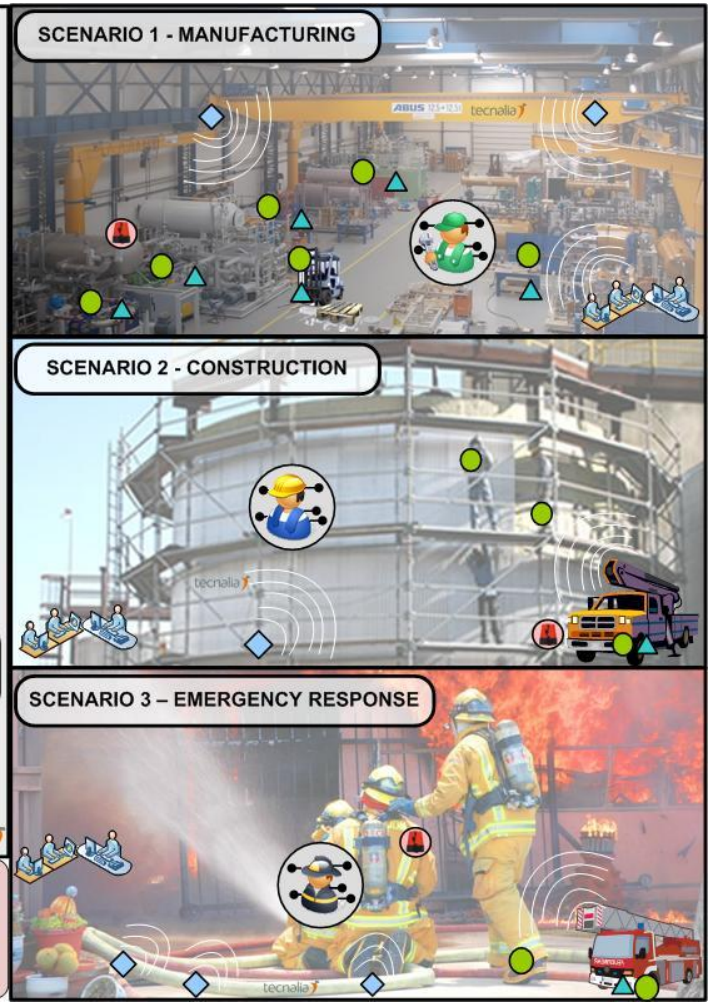
PESI (XV Aniversary): Focused Gps for Horizon Europe

- **OSH (Human & Organizational factors)**
  - **Safety Culture, Health & wellbeing** (Ageing/generational issue, Drugs at work…)
  - **Prevention models** (assistance, aeareness/training serious gaming, pandemics…)
  - **Road Safety at Work, Human factor in Security & CIP (Cybersecurity**, Insider threats)
- **SAFETY under Digital transformation (Industry 4.0/5.0, KET)**
  - **INDUSTRIAL SAFETY** (Smart working environments & Factory 4.0): PPEs, Safety products & systems, Sensoring-Monitoring, NDT, RAMS & Assets Management including ageing)
  - **Structural Safety** (Safe-Infrastructures, in coord. with **Construction & Transport ETPs**)
  - **Civil use of RPAS-drones on Safety-Maintenance & Security** (joint with FG-Sec)
- **SECURITY** (including Industrial **Cybersecurity**)
  - **Governance, Resilience & CIP: Safety-Security-Cybersec Integration (ETPIS)**
  - **Emergencies Management** (jointly with FG-Safety; natural disasters &climate change)
  - **Personnel Security. Technologies for Security; People & Assets Protection**
- **Inter-Platforms Groups:**
  - **CIBERSECURITY** (Information Systems, Industrial Systems)
  - **GICI: Smart, Secure & Resilient Cities**
  - **SAFE MOBILITY**: Tech., ITS, Secure Transport, Hazardous goods transportation
  - **GIEC** (Circular Economy and Sustainabiity)

DISRUPTIV
Plataforma Tecnológica Española de Tecnologías Disruptivas

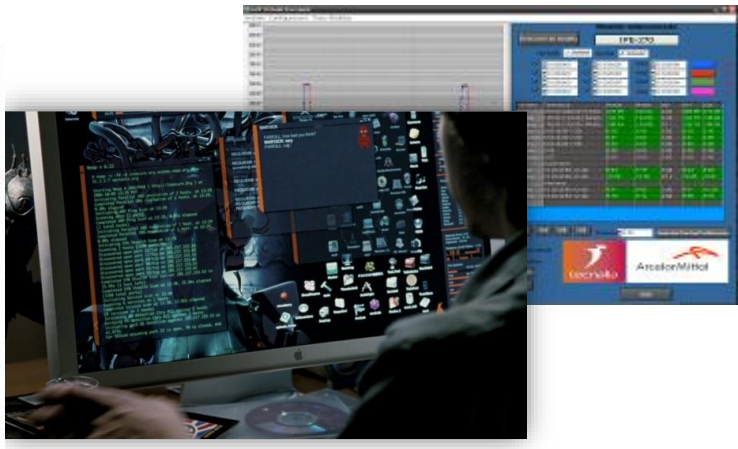
Smart&Safe working environments/Industry 5.0 (Cybersecure)

Digital Factories (**Industry 4.0/5.0):** PPEs (Wearables 4.0), Sensors (IoT), Monitoring (Bigdata, IA), Robotics –colaborative-, VR/AR, **Cyber**, Interoperability (emergencies)



Safe-Infrastructures: vision

- SafeFuture / Safe-Infrastructures vision:
  Safety-Reliability-Resilience 5.0
  - Research towards new concepts and systems, with Safety & Reliability as essential elements in Industrial plants and Utilities networks under Industry 5.0
  - Industrial infrastructures: similar technology & organizational challenges related to ageing >>> common research objetives for safety & reliability
  - **Industrial Control Systems:** also ageing , IT/OT evolution + **cyber-security threats !!**



Complex (Cybersecure) installations: IS, techniques&means

Automation, monitoring, surveillance, O&M (integration of information multi source: sensors, video, bigdata, UAV, Satellite, Machine learning, AI, VR/AR…)



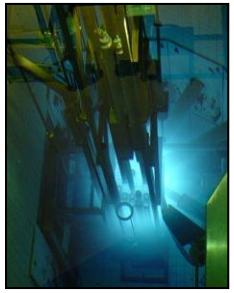


Critical (Cybersecure) infrastructures: special impacts

buried or non-accessible structures

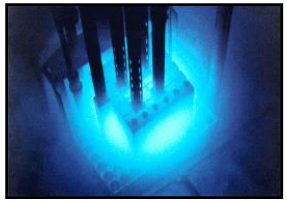


Continuous monitoring of critical areas.

Hazardous or hostile environments



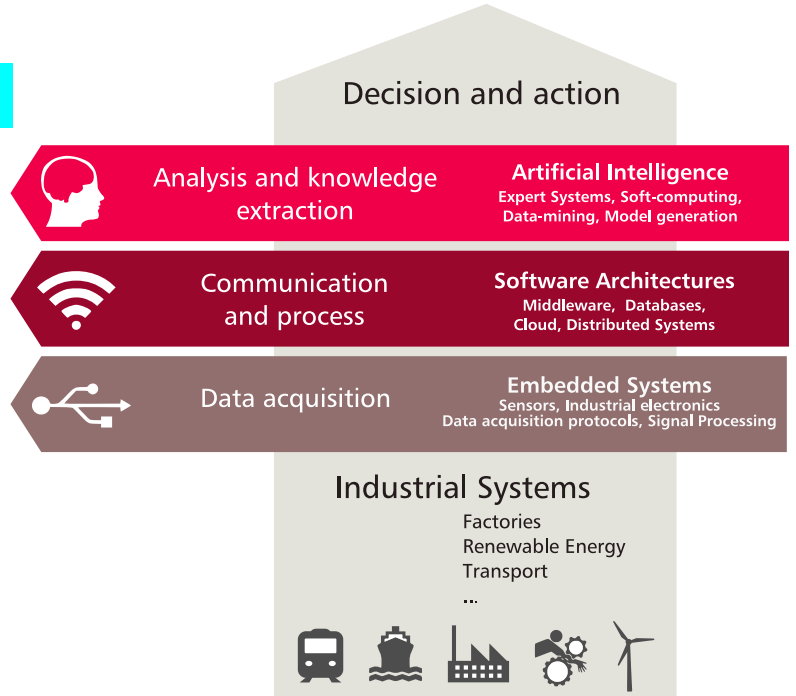


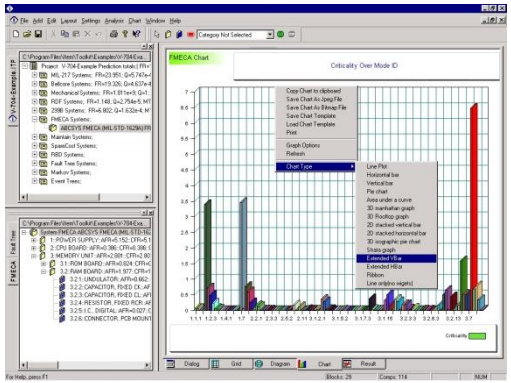

Ageing structures



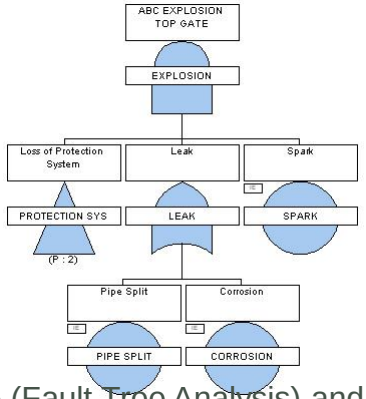
Safety-Security (operation & maintenance)

- **RAMS 5.0** (Reliability, Availability, Maintenance & Safety **+ CyberSecurity** as the reference model
  - **Analysis, Evaluation and Risk Mgt.** (for the whole life-cycle)
  - Predictive Models for maintenance (based on situation: diagnosis, prognosis)
  - Learning from behaviour (Machine Leraning **Artificial Intelligence**). **Digital Twins**.
  - Monitoring&Production integ Systems(PLM.
  - Life-Cycle and **Ageing** Management
  - **ICS Cybersecurity (by design) & Latency**
  - **INFORMATION SYSTEMS 5.0**: IIoT, Big-Data, Cloud, AI, CPS Cyber-physical Systems

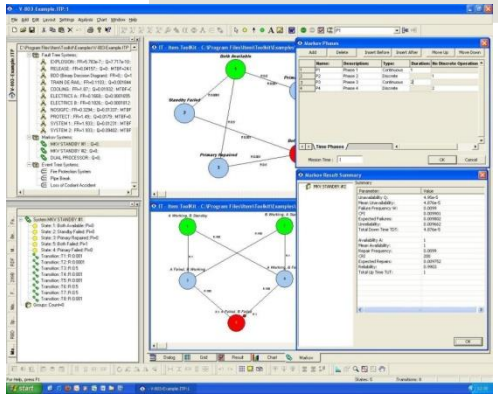




FMECA (Failure Mode, Effects and Criticality Analysis)



FTA (Fault Tree Analysis) and ETA (Event Tree Analysis)



Behaviour modelisation (Markov nets, Altarica,etc…)

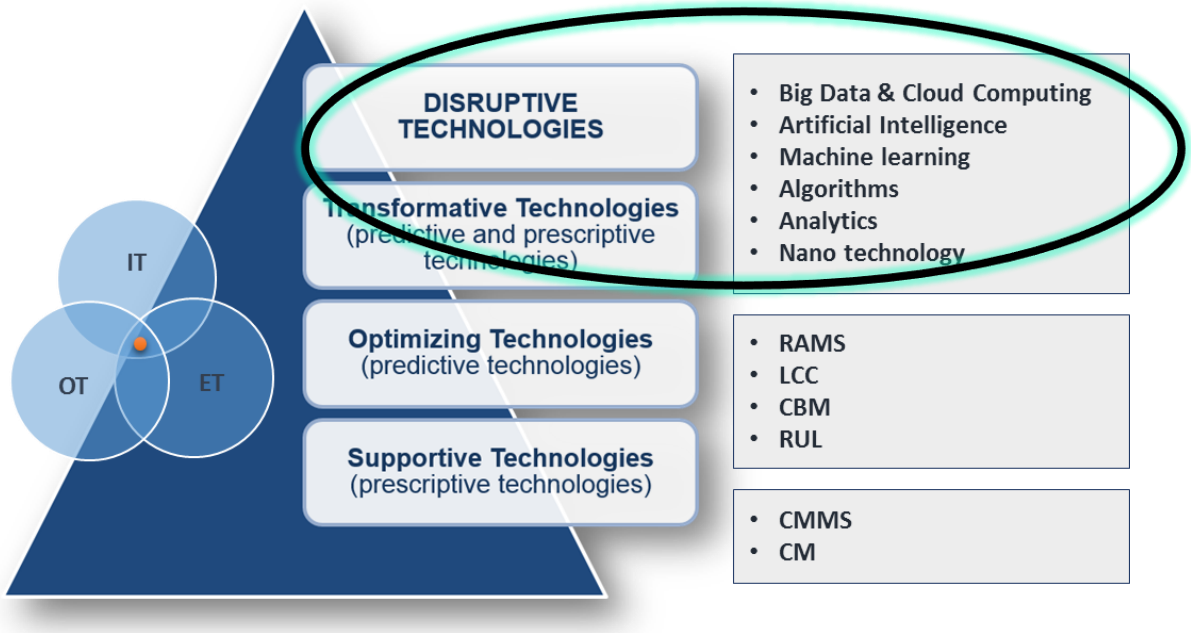
INDUSTRIAL DIGITALIZATION: DISRUPTIVE TECHNOLOGIES FOR RESILIENCE

TRANSFORMATIVE MAINTENANCE SOLUTIONS
Integration & Application of Technologies

Convergencia IT – ET – OT (Cybersecure by design)

Domain knowledge:

- Mining Systems Processes
- Regulations
- Requirement



Información elaborada por: Dr. Diego Galar
Head of Maintenance & Reliability (Div. Industria y Transporte)
diego.galar@tecnalia.com

TECHNOLOGIES FOR WORKER 4.0: REFILOC

Remote monitoring system for Workers safety in plant

Pilot case: REPSOL refinery next to Bilbao

1. Localización de trabajadores en planta: dentro y fuera de espacios confinados
2. Detección de situaciones de emergencia: botón de pánico, “hombre muerto”
3. Detección remota de zonas con atmósferas peligrosas

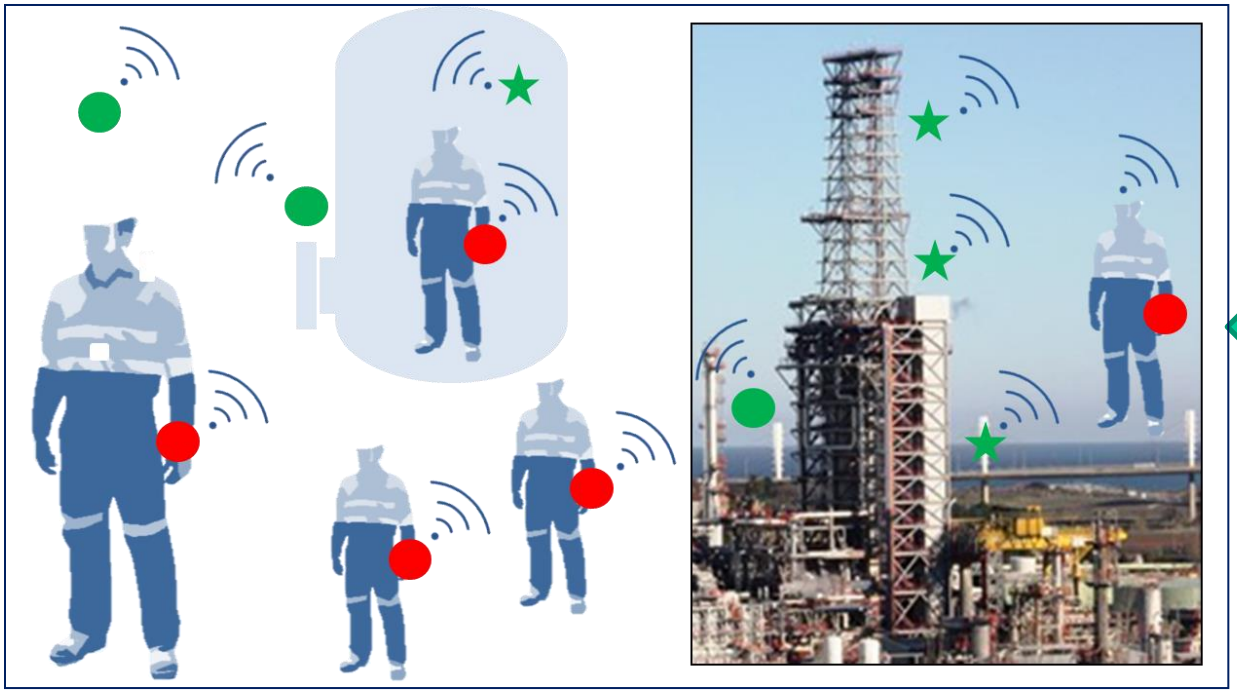
European Technology Platform on
Industrial Safety
Safety for Sustainable European Industry Growth

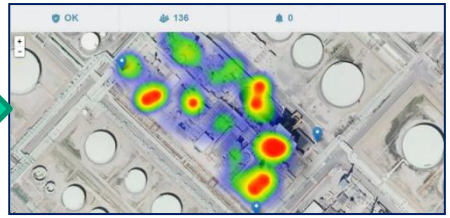
PLATAFORMA TECNOLÓGICA ESPAÑOLA DE SEGURIDAD INDUSTRIAL

SYSTEMS ARCHITECTURE & DEPLOYMENT

REPSOL

tecnalia Inspiring Business





(LEVEL 3. Control Room)

Wearable ATEX bracelets (Level 1) y Balizas (Level 2)
Spread deployment on monitorized area

ATEX bracelet

Baliza-PRO

Baliza-Mini

REFILOC System is based on a 3-Layer architecture: 1) Devices (Wearables), 2) fixed communications infrastructure, spread out through the refinery monitorized area (Balizas) y 3) Control Room (all equipments & devices are ATEX-compliant, Zone 1).

New Governance and integrated Risk Management model (reliability, safety, security and resilience under Industry 5.0 paradigm)

Governance, Integrated Risk Mgt. and Compliance (GRC)

Process & Infrastructures Mgt.: Reliability and Safety (Operation, RAMS, PLM, Maintenance, BIM)

Environmental Safety & Climate change afection

Emergencies Mgt. (Disaster/Crisis Preparation, Civil Protection collaboration)

Safety-Security & Resilience Plans (business continuity, CI dependenc. indicators,…)

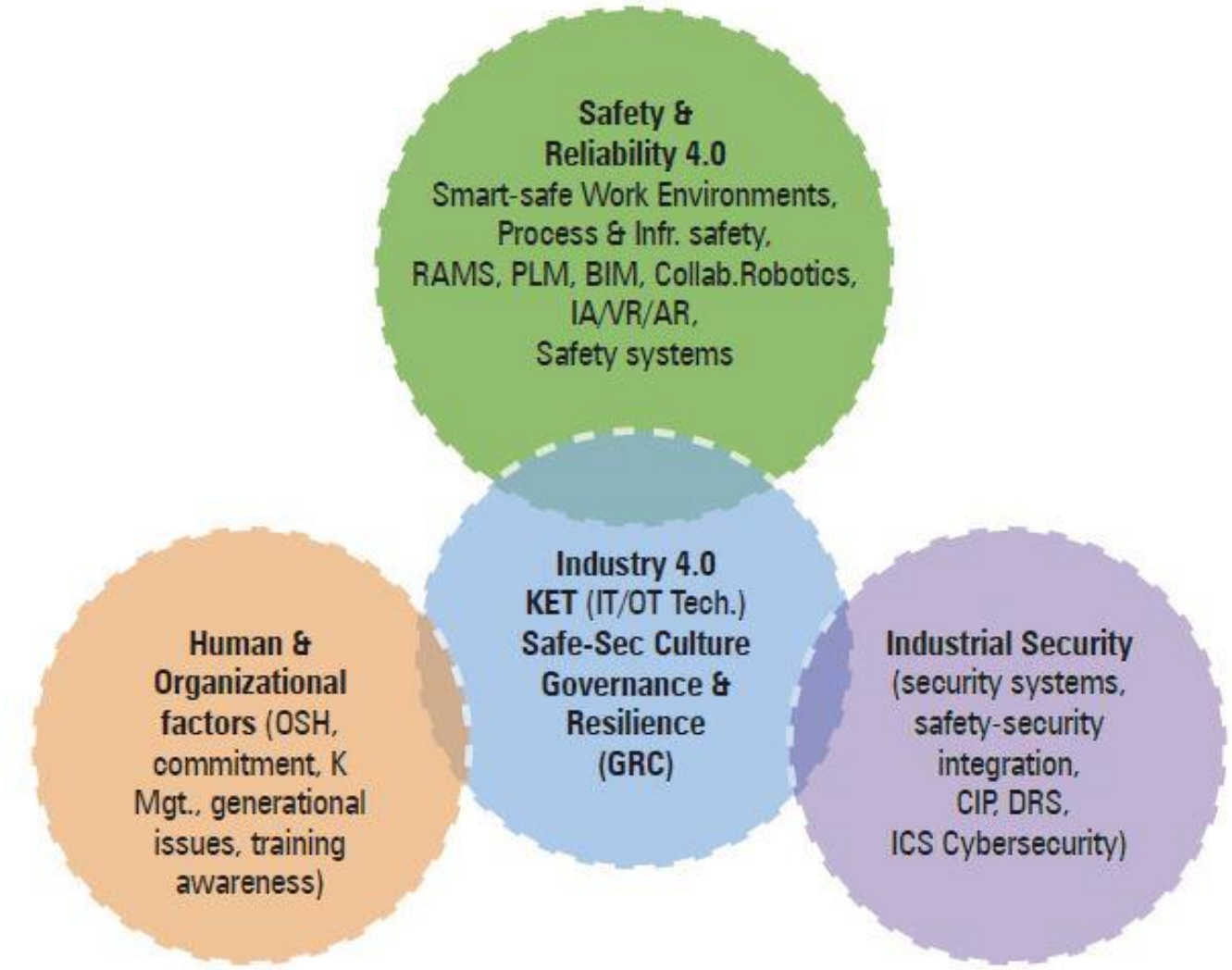
Cyber-Security (Industrial Information Systems)

Corporate Security (protection of staff, infrastructures and K./IP…)

Human Factor in Security (Personnel Security)

OSH: Safe working environments, PPE, safety systems,… (towards corporate wellbeing)

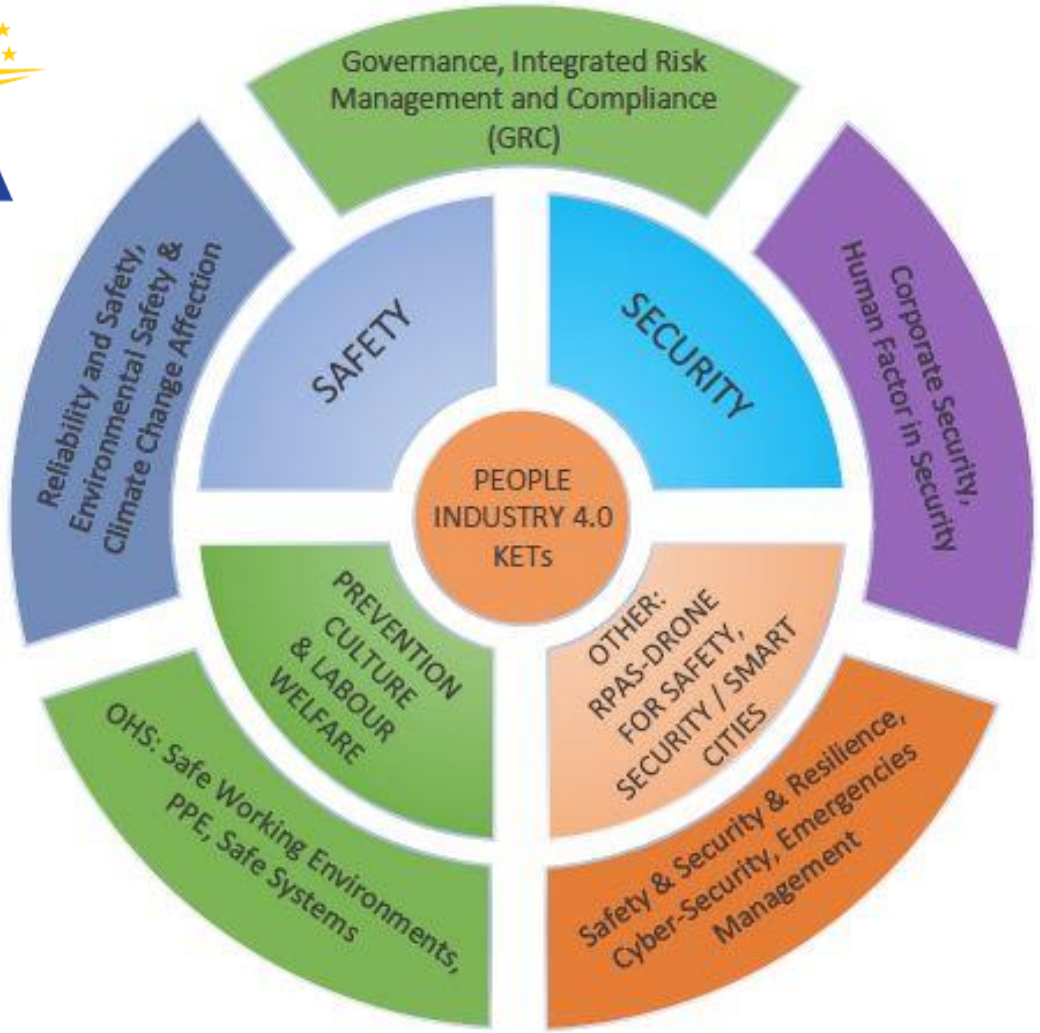
ETPIS: Innovation circles for Horizon Euope (2020)



Security in PESI-ETPIS SafeInfrastructures strategy

- **Safety and Health at work 5.0**(processes, workers)
  - Smart Working Environments (**Worker 5.0, Wearables**…)
  - Civil Protection & Emergencies
- **Asset Management** (ageing infras./extend lifetime, Natural disasters/CC)
  - Sensoring, inspection technologies, structural HMS
  - New materials and smart components (cyber-physical systems…)
  - Engineering techniques, maintenance & repairment
- **Safety and reliability 5.0**:
  - Inherent safety and Risk-based design, Integration (PLM, RAMS, BIM…)
  - Modelling systems, Digital tweens, DSS…
- **IT/OT & Industry 5.0** (technology evolution: challenges & threats)
- **Protection** (critical and non-critical infrastructures)
  - **Security** issues (**Human factor** included)
  - **Cyber-Security** (ICS, SCADA, Wearables…)
- **Governance, Risk Mgt. and Resilience** :
  - **Disasters** (natural, accidents, evacuation, cascading effects on CI)
  - **Dependencies** between **Operators** (resilience, cascading effects)
  - **PPP on Urban Resilience (cooperation with Municipalities/Regions)**

HORIZONTE EUROPA



Security issues and CIP

Security & Resilience related to “Industrial” Critical Infrastructures

Integral Security and Resilience: the new paradigm

- World context: Security and Defence
  - New threats with new means (intelligence, cyber-arms)
- National Strategies (USA, EU) on Security and Critical Infrastructures Protection (CIP) Directives:
  - **Convergence from a National Security (& Defence) vision :**
    - Risk Analysis, physical and logical security plans
    - Military technologies (dual use) for Corporate Security
  - **CIP of "private-operated" critical or relevant Infrastructures (industrial plants / energy / oil & gas/ water/ transport inf.&networks/ telecomms…)**
    - complex industrial installations &infraestructures (more than HQ buildings and IS)
    - Cybersecurity (IS but mainly SCADA)
    - Business Continuity and Resilience
- New driver: Disaster Resilience (climate change increasing nat.disasters)
- **Smart & Secure Cities**: our Citizens and infrastructures are the new target (NY, Madrid, London, Paris, Brussels)

HORIZON EUROPE – Cluster 3 Civil Security for Society 2022 call: R&D topics

SU-INFRA-01: Prevention, detection, response and mitigation of combined physical and cyber threats to critical infrastructures in Europe

- **Critical Infrastructures (for the Smart City)**: Water Systems, Energy Infrastructure (power plants and distribution), Transport Infrastructure and means, Communication Infrastructure, Health Services, Financial Services

SU-INFRA-02: Security for smart and safe cities, including for public spaces

DISASTER RESILIENCE : safeguarding and securing society, including adapting to climate change (Response, Awareness/Civil protection, Communication Systems, Bio threats, CBRN cluster)

DIGITAL SECURITY:

- Cyber Security for SMEs and Individuals, Security Economics, EU and International Coordination in Cybersecurity Research and Innovation, Cyber Security Threats and Threat Actor, Privacy and Data Protection

Horizonte Europa, Cluster 3: INFRA

Addressing interdependencies and systemic risks

Besides the classical approach of protecting infrastructures by sector, a stronger focus on the systemic dimension of attacks is necessary. As such, not only **interdependencies** within one type of infrastructure (or closely related types) can be taken into account, but **large scale disruptions** also with a view of the specific challenges of the cross-border dimension. Specific attention could be dedicated to **Hybrid Threat scenarios**.

- Large-scale Vulnerability Assessments and risks management capabilities, forecasting of emerging risks (via AI)
- Simulations to prepare for systemic disruption of several key infrastructures
- Cross-border scenarios (also with third-countries)
- Better anticipation of systemic risks (including advanced FDI-screening, technological risk assessment)
- Societal resilience against CI-disruption with **Hybrid Attacks** and false news (e.g. finance infrastructure, food-supply and medical system)

Increasing protection and resilience of Critical Infrastructures

Research on CIP is a well-established domain with significant results achieved. Due to the fast evolving technological landscape there are however constantly new challenges and opportunities. **Resilience and Preparedness are keywords to possibly define upcoming research priorities of a cross-cutting nature.**

Example of INFRA R&D proposal: systemic approach (SecureChem: CIP and Dependencies on Chemistry)

Geographical data
Weather
Flood
Energy mix
Transport
Food
Gas network
Seismicity
Heath
Land use & urban planning
Sensitive sites
Ground and underground data
Water systems

existing data bases and periodic reports

CIDER
Critical Infrastructure Disruption Exploration Room

New systems to collect data

Risk & data management

Simulation modules to assess in detail all aspects of interdependent physical, cyber threats and incidents, and the cascading risks resulting

Collect data for prevention, detection, response and mitigation of combined physical and cyber threats to critical

Multi-risk assessment at territory level

Procedures & accident response scenarios at territory level

Steering evidence-based system

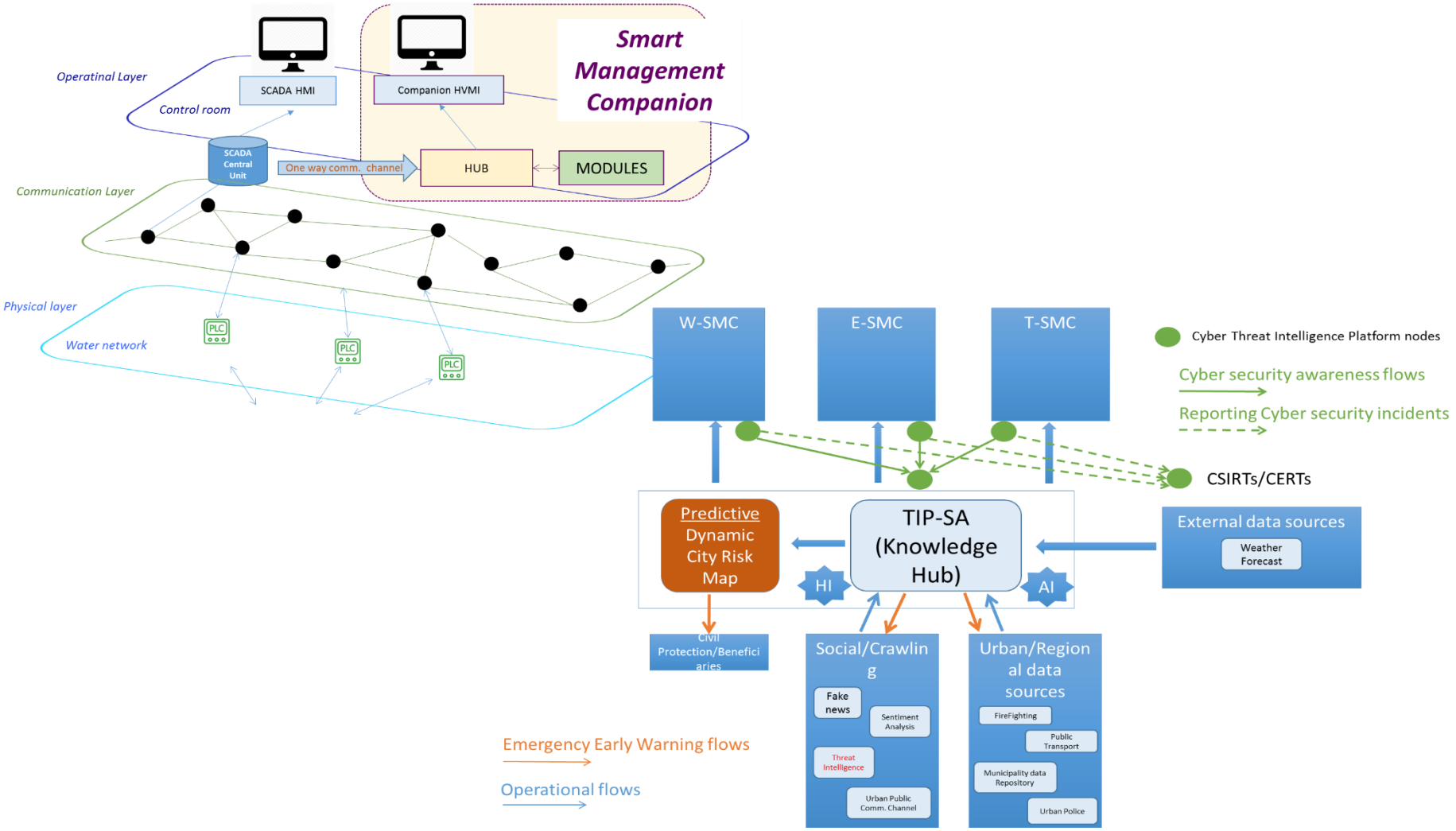
Requirements and recommendations for policy planning, engagement of the civil society, and investment measures

Virtual control room to provide and share a common picture

Geographic information system (GIS) and visual digital system

(decision, coordination, communication)

Example of INFRA R&D proposal: systemic approach (TAU: energy/water systems and Cities)



HE Cluster 3 Cybersecurity – policy priorities

- Network and Information Security – critical infrastructures; CSIRTs/CERTs
- Security certification
- IoT security
- Supply chain security
- Strategic autonomy
- Data protection and privacy (GDPR, ePrivacy)

Cybercrime (FCT topics)

- Cryptocurrencies ([legal as well as technical research]: money laundering techniques, seizure, tracking, fraud committed against legitimate users of cryptocurrencies.
- Child Sexual Exploitation
- Identity theft

HE Cluster 3 Cybersecurity – R&D priorities

Resilient infrastructures and interconnected systems

- Advanced cryptography; quantum
- Automated threat prediction, detection and response
- Human factors – risk and crisis management
- Authentication of IoT objects

Securing disruptive technologies

- Securing AI - 5G - IoT – blockchain – distributed computing
- Big Data privacy

Hardware and supply chain security

- Cryptography and its implementation
- Secure systems, despite vulnerable components
- Virtualisation

Framework for Corporate Security in Spain: National Security Strategy & CIP Law

Deployment of the National CIP Law (CNPIC):

- Sectors & Critical Infrastructures :
  - Private Operators
  - Public Administrations
- Sectoral White-Books (13: 8 industry-related)
- PSO Operator Security Plan
- PPE Specific Protection Plans (individual CIs)
- Entreprise Security Organization and Plans
  - New integrated Strategy & Risk management (adaptation of Saf-Sec systems & plans)
  - Certification of Sec plans/systems (CNPIC)

+ New Law for Security Private Services (security subcontractors in Operators)

Systems and Technology towards Resilience

- Organization and new responsabilities in Safety & Security
  - **Integrated Risk Analysis** & Business Intelligence (TS/CI, new risks: conflicts and radicalization)
    - Operational Reliability and Safety (engineering / process): industrial and environmental Safety and OSH
    - Security-Cybersec of industrial installations, infrastructures and networks
    - Information Security (IT-OT: Cybersecurity)
  - **GRC Strategy** &organization based on a real **SECURITY-SAFETY integration**
- New Framework (**CIP/NIS2 Directive** & National Laws, EU Goals and Resilience, Horizon Europe-Cluster3/Security):
  - **Convergence safety- security** (from different visions: industrial safety, cybersecurity and corporate security): integrated **Risk Mgt./Dependencies**
  - **DRS** (**Natural Disasters Resilience, including climate change**) and Tech. Accidents (Civil Protection and emergencies plans): **Crisis Mgt**.
  - Critical Infrastructures **Protection** (industry / utilities/ transport…) towards **BC**
  - **Cybersecurity** by design (IS security, automation&control systems/SCADA)
  - **Business (essential services) Continuity and Resilience**

PESI integrated approach

Risk Management, Business Continuity and Resilience (considering Dependencies)

Risk Management and Risk concept evolution

Conventional Risk concept:

- Threat / hazard – Vulnerability – Consequences

Risk Management (ISO 31000)

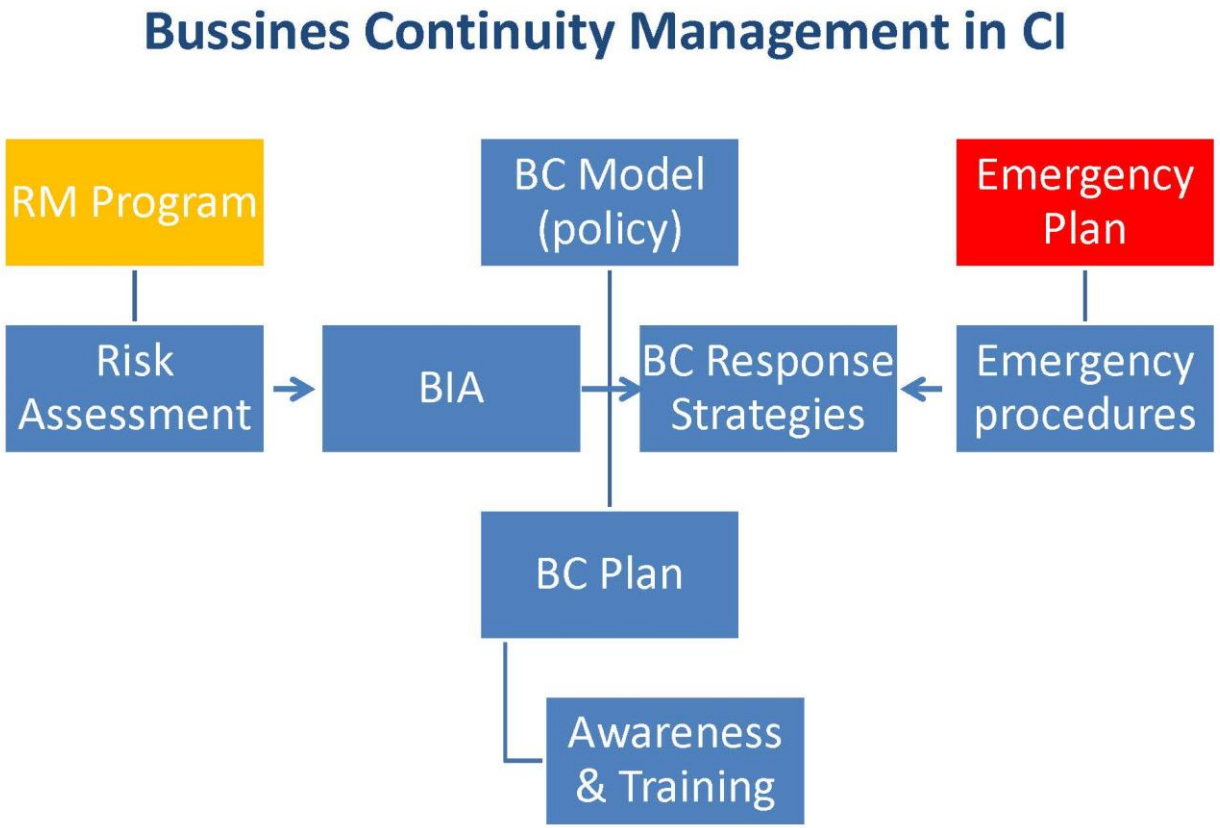
Resilience capability in an advanced Risk concept:

- Threat / hazard – Vulnerability – **Resilience** – Consequences
- Resilience: Processes/Systems/Services

Resilient People (2 layers: Individual & Teams)

PESI integrated approach for BC and Resilience in CI

Integrated Risk Management and Emergency Mgt. within an advanced Business Continuity Model



RA and BIA (Dependencies assesment)

- **Risk and Dependencies Assesment:**
  - Functions and Services evaluation (criticity level)
  - Resources (requirements):
    - Personnel
    - Equipment
    - SW systems, ITC, **Cybersecurity**
    - Utilities (Inter-dependencies)
    - Materials …
- **Business Impact Analysis:**
  - Intra-dependencies
  - Inter-dependencies (external CIs)
  - Cascading effects (up-stream & down-stream)

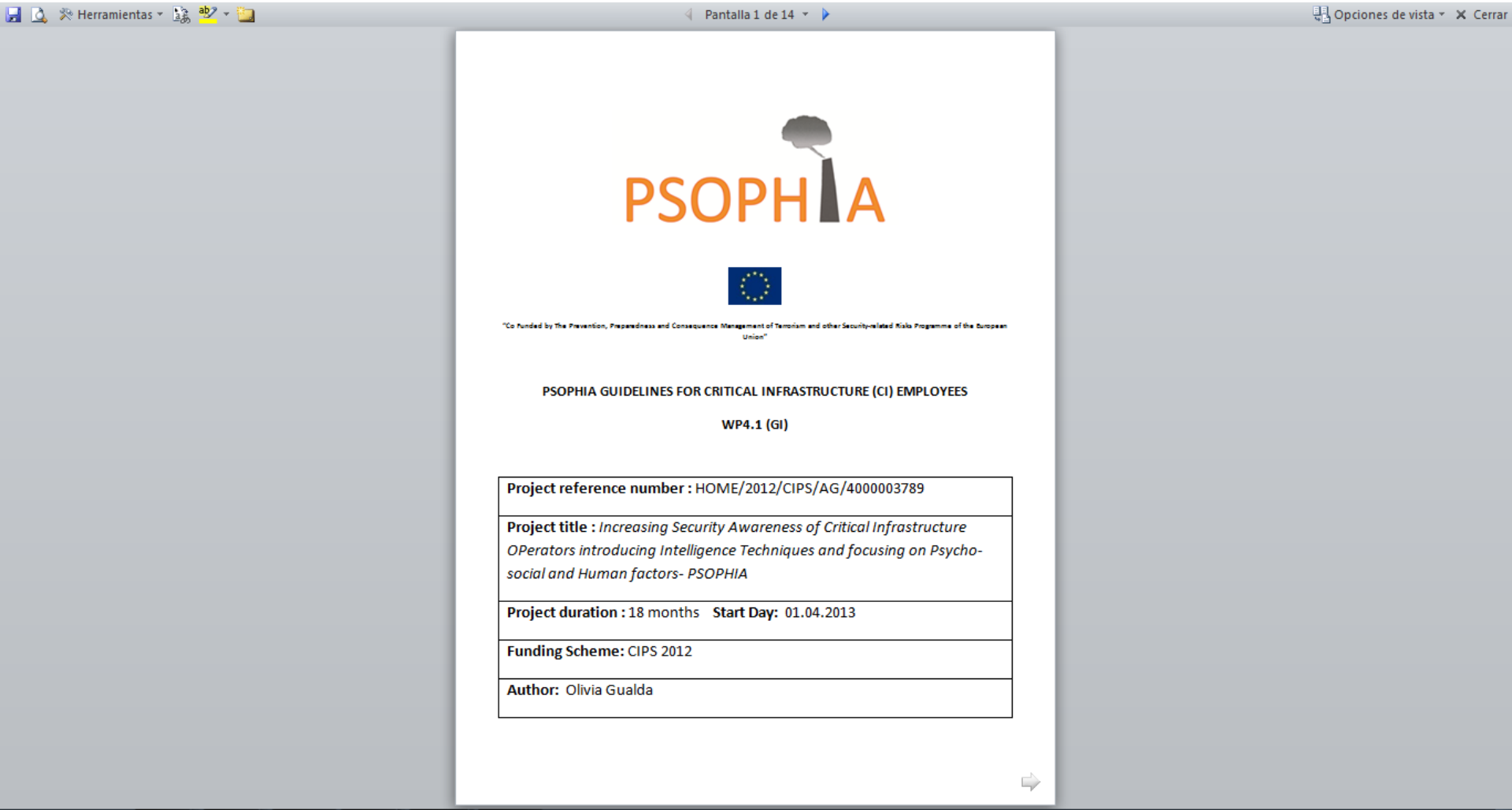
Criticity evaluation (10 categories) and Dependencies

Categories	Critical Elements of the CI	INTRA-DEPENDENCIES	Direct Impacts	Control Rooms (Operation)	Security Control Rooms	Info Systems (OT/IT, ciber) &Comm	Staff - Mgnt Board & Crisis Committee	Essential Teams	other staff & ext personnel	Critical Proc-1	Critical Proc-2	Critical Proc-n	Security Equipment & Systems	(essential) Equipment & appliances	Infraestructures (buildings)	External Services &Supplies	Others
I	Control Rooms (Operation, Security, Integral)			■													
I	- Security Control Rooms				■												
II	Information Systems (OT/IT, ciberseg.) &Communications (voice, radio, IP...)																
III	Staff - Mgnt Board & Crisis Committee																
III	- essential Teams (Op&Maint, Emerg, ITC)																
III	- other personnel & subcontractors																
IV	Critical Processes (industrial/essential service, restricted areas...; safety systems)									■							
IV	Critical Process-2										■						
IV	Critical Process-n											■					
V	Security Equipment & Systems																
VI	Equipment & appliances (esential)																
VII	Infraestructure (buildings, installations)																
VIII	External Services &Supplies (Subcontr&Providers)																
IX-X	Others (economic, legal, Soc accept., specific)																

Inter-dependencies (critical elements) with external CI

	INTER-DEPENDENCIES	Direct Impacts	Energy	Gas/oil	Water	Telecoms (voice, data &ISP)	Location & Environment	Transport Infrast. (road, train	Logistics (& purveyance)	Security, Civil Protection & Emergencies	Others
Categories	Critical Elements of the CI										
I	Control Rooms (Operation, Security, Integral)					5					
I	- Security Control Rooms					5					
II	Information Systems (OT/IT, ciberseg.) &Communications (voice, radio, IP...)					5					
III	Staff - Crisis Committee										
III	- essential teams (Op&Maint, Emerg, ITC)							4			
III	- other personnel & subcontractors										
IV	Critical Processes (industrial/essential service, restricted areas...; design, organization, tasks, safety systems)										
IV	Critical Process-2								4		
IV	Critical Process-n										
V	Security Equipment & Systems										
VI	Equipment & appliances (esential)										
VII	Infraestructure (buildings, installations)						2	2			
VIII	External Services &Supplies (Subcontr&Providers)										
IX	*Economic & Legal (Stability); Societal acceptance*										
X	Others (specific in the CI)										

PESI contribution to CI Security: PSOPHIA (Personnel Security & Social Engineering HUMINT)



PSOPHIA

"Co Funded by The Prevention, Preparedness and Consequence Management of Terrorism and other Security-related Risks Programme of the European Union"

PSOPHIA GUIDELINES FOR CRITICAL INFRASTRUCTURE (CI) EMPLOYEES

WP4.1 (GI)

Project reference number : HOME/2012/CIPS/AG/4000003789
Project title : *Increasing Security Awareness of Critical Infrastructure OPerators introducing Intelligence Techniques and focusing on Psycho-social and Human factors- PSOPHIA*
Project duration : 18 months **Start Day:** 01.04.2013
Funding Scheme: CIPS 2012
Author: Olivia Gualda

Final recommendations

CI Operators cooperation & Resilient Cities

Inter-dependencies: cooperation between CI Operators

- **CI Operators: Security and Resilience Plans** developed evaluating the main and direct **dependencies** and considering other "theoretical inter-dependencies" (defined by the strategic sectoral security plans coordinated by Governments and Operators)
  - Enlarg depedencies Ass. based on an in-detail analysis for all active elements in the CI network/system (previous experiencies…)
  - Sec Plans and related information "classified" or "restricted"
  - Difficulties for sharing relevant information
- Build ***spaces for confidence***: e.g. CERT and Technical Committees (led by National Agency for CIP) for CI Operators Security Dpts.
- Resilience **Exercices** (CI Operators in collaboration) **and Cyber-exercices**

Urban Resilience and Safe CI Operators

- **Community** requirements for availability and *resilience of the essential services* (CI) at Local and Regional levels
- Public **contracts** (concessions) for Utilities and other public services operated by private companies: include clauses for *QoS and "resilience" plans to the Operators*
- New **collaboration** schemes between CI Operators and Municipalities and Regional Governments (PPP for Security and Resilience)

Ámbitos de Seguridad Corporativa y Protección de Infraestructuras (industriales, redes, ciudad)

Security y PIC, Operación, Ciberseguridad y Resiliencia

SERVICIOS DE APOYO A CONSORCIOS Y PROPUESTAS

- **Búsqueda de Socios adecuados**
  - Empresas y Operadores de ICs
  - PYMES tecnológicas e Ingenierías
  - Socios Europeos (red ETPIS2 y Asociaciones sect./Investigación)
  - Expertos para IAB (Advisory Board, Int. Committees…)
- **Impacto. Análisis y Explotación de Resultados**
- **Apoyo en la diffusion (Jornadas europeas…)**

TOPICS DE INTERÉS (Horizonte Europe Cluster-3 Seguridad)

- **Resilient Infrastructures** (**INFRA** topics)
- **Increased cybersecurity** (**CS** topics)
- **Disaster-Resilient Society for Europe** (**DRS** topics)

Muchas gracias / Eskerrik asko
Thank you so much.

J. Javier Larrañeta, Secretario General
javier.larraneta@tecnalia.com
secretario-tecnico@pesi-seguridadindustrial.org

XIV Aniversario PESI

PLATAFORMA TECNOLÓGICA ESPAÑOLA
DE SEGURIDAD INDUSTRIAL

Thank you so much for your attention:

Questions or comments ?

J. Javier Larrañeta
PESI Secretary General
javier.larraneta@tecnalia.com
secretario-tecnico@pesi-seguridadindustrial.org