



Cyber-risks as a threat to critical infrastructures and the functioning of Switzerland

National Cyberstrategy and countermeasures by FONES

Daniel Caduff

Federal Office for National Economic Supply FONES

Deputy Head of Secretariat ICT Division



Mandate



- Federal Constitution of the Swiss Confederation Art. 102
- National Economic Supply Act
- Mandate to increase the resilience of supply infrastructure



CIP vs. Supply-Chain-Perspective

| | | Resources | Preliminary work |
|--|------------|-----------|------------------|
| Supply Processes of the vital goods and services | Energy | | |
| | Food | | |
| | Healthcare | | |
| | Logistics | | |
| | ICT | | |

- ICT is a critical service by itself
 - Telecommunication infrastructure
- ICT is also a critical resource for other sectors
- Necessity to secure both: the critical telecommunication infrastructure, as well as the critical ict-resources for other sectors
- Interdependency is rising with automation.
- A more Supply-Chain-oriented perspective is necessary. Nevertheless: Risk appetite needs to be defined. i.E: Electricity in Switzerland: Maximum acceptable loss: 50 GWatt



Shared and distributed responsibility in the area of cyber



Duties:

- Cyberdefence (Departement of Defence, Civil Protection and Sport)
- Cybercrime (Departement of Justice and Police)
- Cybersecurity / Critical infrastructure protection (Multiple departements)
- Organisational separation, but close cooperation



Real-life example: Attack on the water-supply of a Swiss municipality

Abn

«Hacker haben unsere Wasserversorgung angegriffen»

Ebikon meldete jüngst eine IT-Attacke. Wie gefährdet ist unsere Infrastruktur wirklich? Diese Lecks und Schwachstellen könnten zur Bedrohung werden.

Beat Metzler, Christian Zürcher
Aktualisiert: 12.03.2019, 23:43



Unpraktisch, aber sicher vor Hackern: Walter Zürcher erklärt die analoge Wasserversorgung von Schwarzenegg. Foto: Christian Pfander

- In 2018, an attack against a Swiss water utility (municipality of Ebikon) became known.
- The attack was not successful, but showed that even smaller operators of critical infrastructures can nowadays become the target of cyber attacks.
- Since the attack was directed against the control systems, there was also a supply risk for the population.
- Such attacks are particularly critical for interconnected companies that are responsible for several supply processes (e.g., electricity, water, natural gas).



Real-life example: Cyberattack on a Swiss hospital (one of many attacks)



Krankenhäuser geraten zunehmend ins Visier von Cyberkriminellen.

«Gefährlichste Malware der Welt» attackiert Zürcher Spital – das musst du wissen

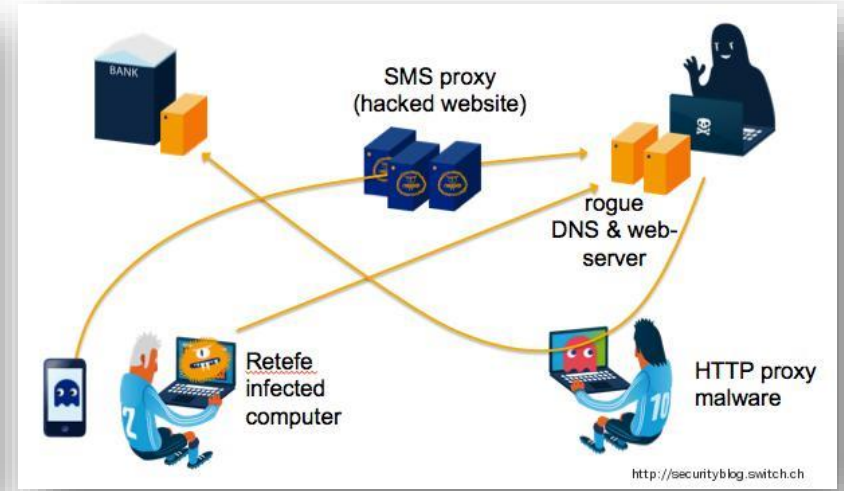
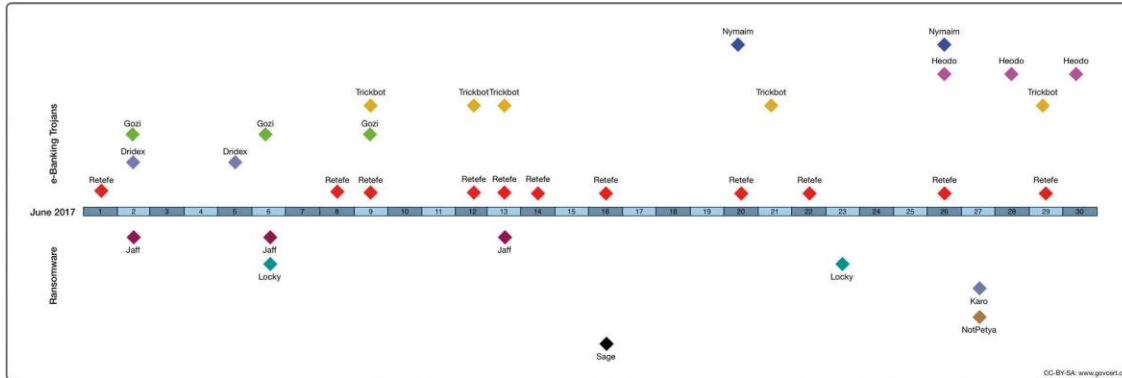
Fachleute bezeichnen Emotet als derzeit gefährlichste Schadsoftware der Welt. Kürzlich hat es ein Spital im Kanton Zürich erwischt. Hier sind die wichtigsten Fragen und Antworten rund um den Cyberangriff.

- Unlike other critical infrastructure, hospitals are openly accessible
- There are systems, such as heart-lung machines, where cyberattacks are potentially lethal to patients.
- A hospital sometimes has hundreds of different devices from different manufacturers in use. Maintenance and oversight are extremely difficult.
- Certification of medical devices prohibits subsequent modification of software no updates possible.
- In hospitals, critical systems are often operated by doctors and nurses. Not by cyber professionals.



Real-life example: Banking Trojans

- Most often, not banks are attacked, but customers
- Combination of various techniques: Technical (i.e. Keylogger, MiM, RATs) and social (Social Engineering, Phishing)
- Lots of banks pay, but demand secrecy



ICT minimum standard



- The standard is generic and universally applicable
- It's primary focus is on critical infrastructures
- The standard specifies *what* to do, but leaves the user the freedom to decide *how* he wants to do it
- The standard is based on the NIST-Framework, but compatible with other industry standards, such as ISO, Cobit, ITIL...



How does the standard work?



- Developed by FONES with experts from the National Economic Supply (Private Sector)
- 5 chapters, each with designated chapters.
- 106 activities in total. Rating from 0 to 4.



Example: Adaption for the food-sector (1/2)



- Businessprocess-analysis, including identification of actors
- Identifying mission-critical tasks
- Identifying ICT-dependencies of mission-critical tasks
- Identifying vulnerabilities



Example: Adaption for the food-sector (2/2)

Critical tasks



- Production
- Logistics



- Orders
- **Processing & packaging**
- Storing
- Picking
- Distribution
- Communication



- **Order**
- Import
- Goods management (ERP)
- **Selling (POS)**
- Communication

ICT-Systems

- Feeding systems
- Phone
- ERP (SAP)
- SCADA
- SCADA
- Picking System
- Touring-Planing-System
- Phone and mail
- Point of Sale (checkout)
- ERP (SAP)
- Inventory management
- Phone and mail

Vulnerability-Score

| K | G | A | R | V |
|---|---|---|---|-----|
| 3 | 3 | 1 | 1 | 9 |
| 5 | 1 | 1 | 1 | 5 |
| 3 | 3 | 3 | 1 | 27 |
| 5 | 3 | 5 | 3 | 225 |
| 3 | 3 | 5 | 1 | 45 |
| 3 | 3 | 3 | 1 | 45 |
| 5 | 3 | 3 | 1 | 45 |
| 5 | 1 | 5 | 3 | 75 |
| 5 | 3 | 5 | 3 | 225 |
| 5 | 3 | 3 | 1 | 45 |
| 5 | 3 | 5 | 1 | 75 |
| 5 | 3 | 5 | 3 | 225 |
| 5 | 1 | 5 | 3 | 75 |

K = Kritikalität, G = Gefährdung, A = IKT-Abhängigkeit, R = Resilienz, v = Verwundbarkeit

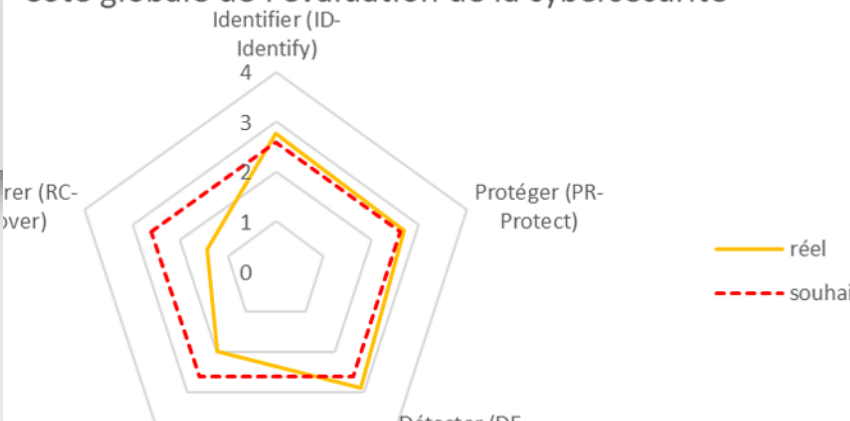


How does the standard work?

Norme minimale TIC - Outil d'évaluation

| Thème | Catégorie | Tâches | Appréciation | Commentaires |
|--|-----------|---|--------------|--|
| Inventaire et organisation (Asset Management) Les données, les personnes, les appareils, les systèmes et les installations d'une entreprise sont identifiés, catalogués et évalués. L'évaluation de leur criticité pour les processus opérationnels à mettre en place et de la prise en compte de la gestion des risques. | | ID.AM-1: Développez un processus d'inventaire garantissant en permanence un recensement exhaustif de vos équipements TIC (Asset). | n/a | CCS CSC COBIT 5 E ISA 62443-1 ISA 62443-2 ISO/IEC 27001 NERC CIP BSI-Standard Anwendung NIST SP 800-53 |
| | | ID.AM-2: Inventoriez toutes les plateformes, licences et applications logicielles dans votre entreprise. | n/a | CCS CSC COBIT 5 B ISA 62443-1 ISA 62443-2 ISO/IEC 27001 NERC CIP BSI-Standard Anwendung NIST SP 800-53 |
| | | ID.AM-3: Listez tous les flux de communication et | n/a | CCS CSC COBIT 5 D ISA 62443-1 ISO/IEC 27001 |

Cote globale de l'évaluation de la cybersécurité

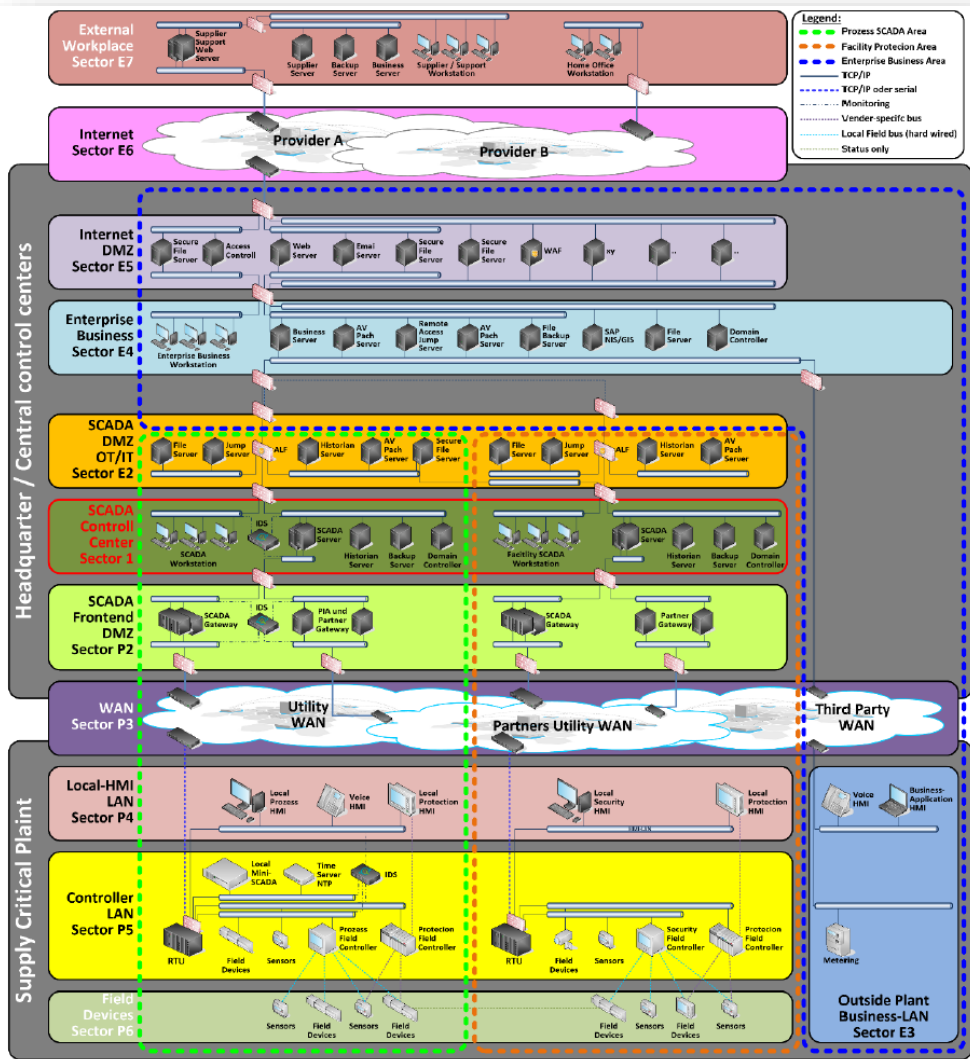


- Excel-based assessment-tool available (Open Source, free for everyone).
- 106 activities, to be rated from 0 – 4 .
- The standard is risk-based, scalable and auditable.
- Compatibility to various industry-standards (ISO, IEC, ITIL, COBIT...)
- → To be replaced by a webbased tool (work in progress)



Example: ICS / SCADA – Security for the electricity supply

- Recommended network architecture and segmentation
- Different segments with predefined communication table



Interne Verbindungsmatrix für die den Sektor P5 Basic Control in einer versorgungskritischen Anlage

| von \ nach | | Central Control Centers | | | | | | | Supply Critical Plant | | | | Local HMI | |
|-------------------------------|----------------------|-------------------------|-----------------|-----------------|-----------------|-----------------|--------------------|--------------------|-----------------------|---------------------|---------------------|-------------------------------|-----------------|-------------------------------|
| | | Gateway | Gateway | Gateway | Field Device 1 | Field Device 2 | Field Controller 1 | Field Controller 2 | Field Sensor 1 | Protection Sensor 1 | Protection Sensor 2 | Protection Field Controller 1 | | Protection Field Controller 2 |
| Direction | Direction | Direction | Direction | Direction | Direction | Direction | Direction | Direction | Direction | Direction | Direction | Direction | Direction | Direction |
| Gateway | Direction Field | x | Nein | Nein | tcp/102 udp/123 | tcp/102 udp/123 | tcp/102 udp/123 | tcp/102 udp/123 | Nein | Nein | Nein | Nein | Nein | |
| Gateway | Direction Protection | Nein | x | Nein | Nein | Nein | Nein | Nein | tcp/102 udp/123 | tcp/102 udp/123 | tcp/102 udp/123 | tcp/102 udp/123 | Nein | |
| Gateway | Direction HMI | Nein | Nein | x | Nein | Nein | Nein | Nein | Nein | Nein | Nein | Nein | tcp/102 udp/123 | |
| Field Device 1 | Direction Field | tcp/102 udp/123 | Nein | Nein | x | tcp/102 udp/123 | tcp/102 udp/123 | tcp/102 udp/123 | Nein | Nein | Nein | Nein | Nein | |
| Field Device 2 | Direction Field | tcp/102 udp/123 | Nein | Nein | tcp/102 udp/123 | x | tcp/102 udp/123 | tcp/102 udp/123 | Nein | Nein | Nein | Nein | Nein | |
| Field Controller 1 | Direction Field | tcp/102 udp/123 | Nein | Nein | tcp/102 udp/123 | tcp/102 udp/123 | x | tcp/102 udp/123 | Nein | Nein | Nein | Nein | Nein | |
| Field Controller 2 | Direction Field | tcp/102 udp/123 | Nein | Nein | tcp/102 udp/123 | tcp/102 udp/123 | tcp/102 udp/123 | x | Nein | Nein | Nein | Nein | Nein | |
| Field Sensor 1 | Direction Field | tcp/102 udp/123 | Nein | Nein | tcp/102 udp/123 | tcp/102 udp/123 | tcp/102 udp/123 | Nein | x | Nein | Nein | Nein | Nein | |
| Protection Sensor 1 | Direction Protection | Nein | tcp/102 udp/123 | Nein | Nein | Nein | Nein | Nein | x | tcp/102 Goose | tcp/102 Goose | tcp/102 Goose | Nein | |
| Protection Sensor 2 | Direction Protection | Nein | tcp/102 udp/123 | Nein | Nein | Nein | Nein | Nein | tcp/102 Goose | x | tcp/102 Goose | tcp/102 Goose | Nein | |
| Protection Field Controller 1 | Direction Protection | Nein | tcp/102 udp/123 | Nein | Nein | Nein | Nein | Nein | tcp/102 Goose | tcp/102 Goose | x | tcp/102 Goose | Nein | |
| Protection Field Controller 2 | Direction Protection | Nein | tcp/102 udp/123 | Nein | Nein | Nein | Nein | Nein | tcp/102 Goose | tcp/102 Goose | tcp/102 Goose | x | Nein | |
| Local HMI | Direction HMI | Nein | Nein | tcp/102 udp/123 | Nein | Nein | Nein | Nein | Nein | Nein | Nein | Nein | x | |



Resilient Public Transport Systems

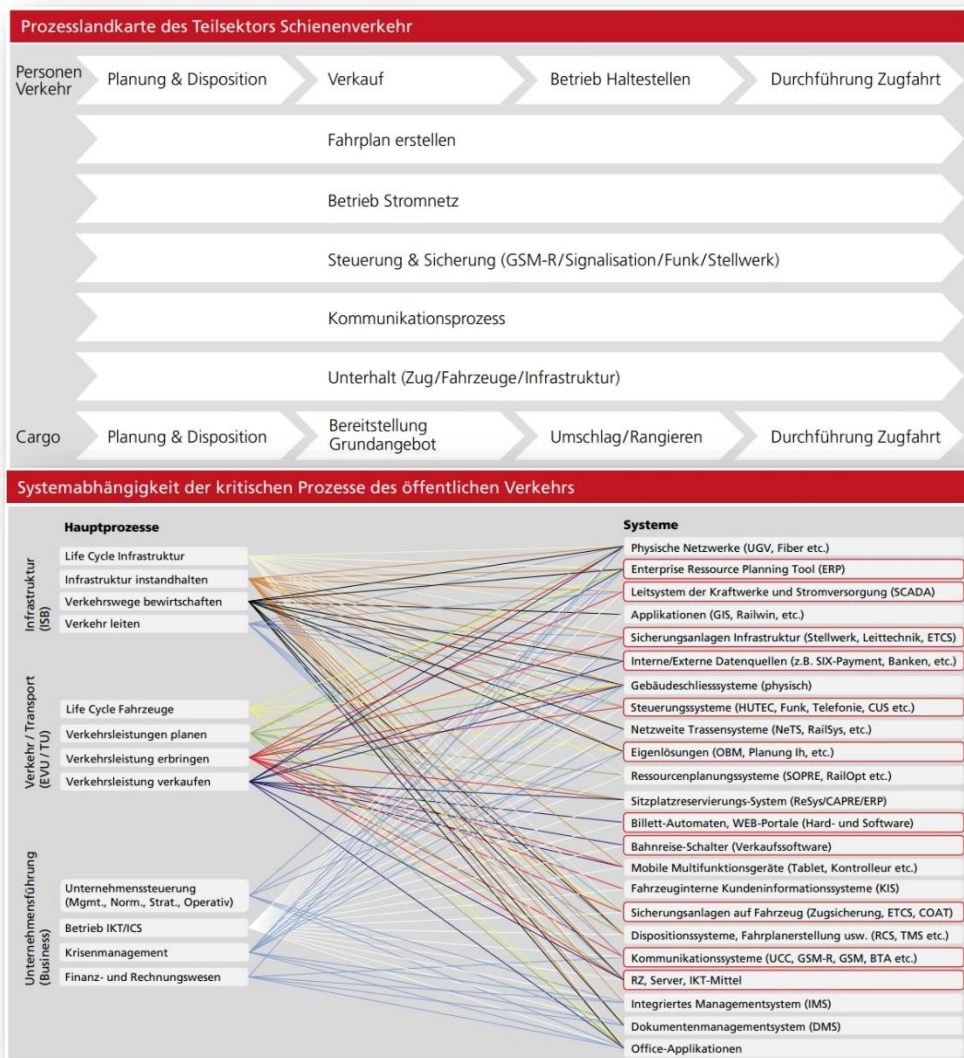
Example: Strengthening availability of ICT-infrastructure



- ICT Minimum to strengthen resilience in public transport
- Identification of processes, vulnerabilities and risks
- Raising awareness
- Prevention: Reduce risk-probability
- Resilience: Preparedness, measures, training
- Identify, Detect, React, Respond, Recover
- Security is not a state to achieve, but a constant process
- Developed in cooperation between private sector and federal office → Public Private Partnership



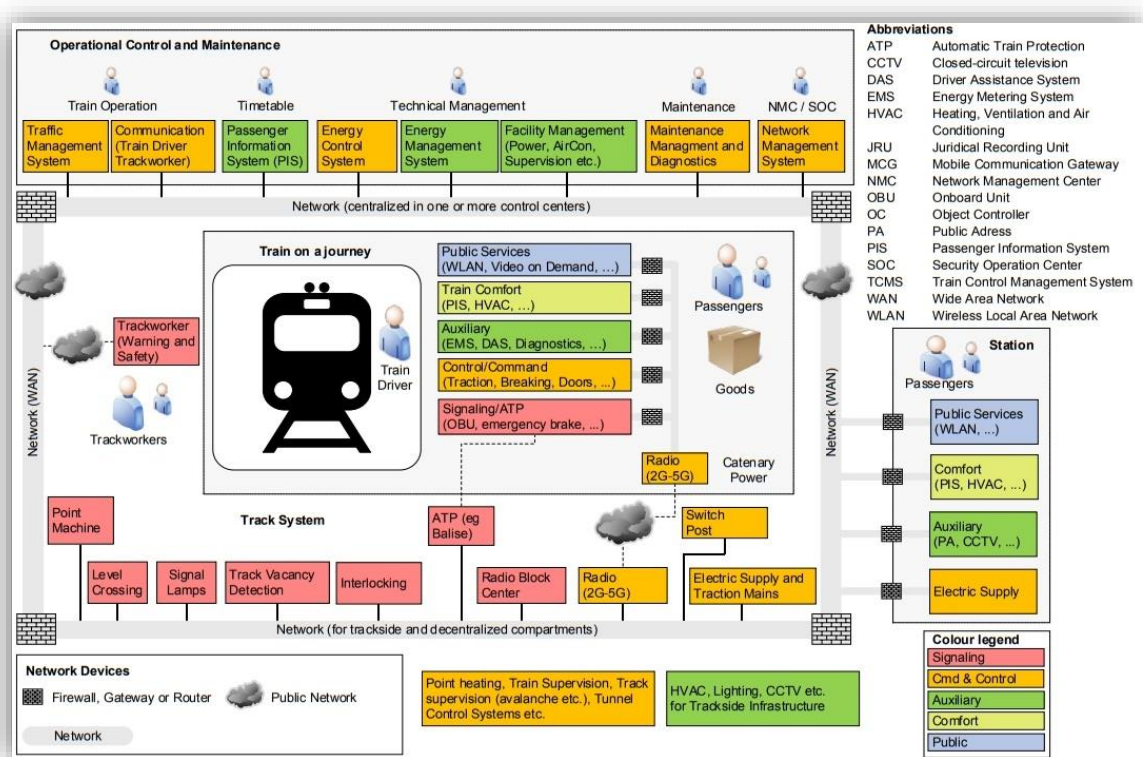
Resilient Public Transport Systems: How to



- Evaluation of (core)processes and actors
- Evaluation and documentation of dependencies between critical processes and critical ICT-resources
- Know your assets, know your critical systems and dependencies
- “Learning by doing” → Developing standards helps to ask the right questions and to raise awareness.



Resilient Public Transport Systems: How to



- Leverage generic ICT Minimum Standards into detailed network segmentation
- Public Transport Systems are connected systems over various enterprises, regulators and even nations
- Integrate cybersecurity into groupwide risk-management
- Safety > Security



Resilient Civil Communications Systems

Example: Strengthening availability of ICT-infrastructure

The screenshot shows the OFCOM website with the following content:

- Navigation: The Federal Council > DETEC > OFCOM
- Search: Search bar and Glossary dropdown
- Menu: Digitalisation and Internet, Telecommunication, Electronic media, Frequencies and antennas, Equipments and installations, OFCOM
- Breadcrumbs: Homepage > OFCOM > OFCOM's information > Press releases > Mobile networks require better protection against power outages
- Left sidebar: OFCOM, OFCOM's information, Press releases, OFCOM Press Service, OFCOM Infomailing, Newsletter No 407 (01.02.2021), Annual reports, Newsletter and social media
- Main content:

Mobile networks require better protection against power outages

Bern, 04.12.2020 - Operators of mobile telecommunication networks need to take additional measures to ensure that the population and economy can continue to use essential mobile services during a power outage. This is the conclusion of a study by the Federal Department of the Environment, Transport, Energy and Communications, which the Federal Council took note of at its meeting on 4 December. In a first step, the Federal Council wants to ensure that there is no disruption to the emergency services during a power outage.

The complete text is available in German, French and Italian. Please click on the desired language in the navigation menu above.

Address for enquiries

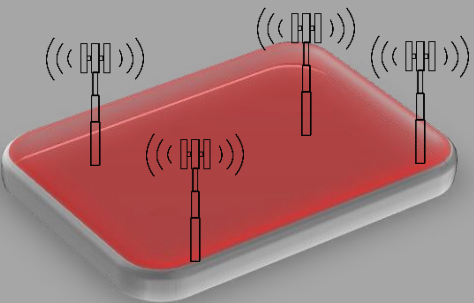
Federal Office of Communications (OFCOM), Press Service, +41 58 460 55 50, media@bakom.admin.ch

- Preparation against power outages
- Evaluating several possibilities to ensure power supply
- Defining key-infrastructure elements to ensure minimum coverage (→ need to be resilient!)
- Combination with other measures possible: i.e. Priority-Scheme



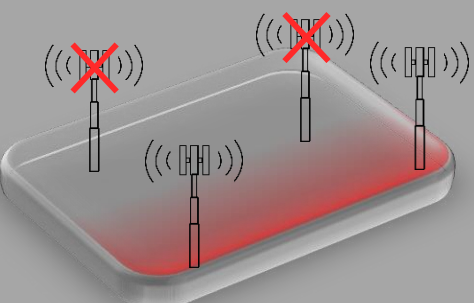
Resilient Civil Communications Systems: How to

Normal state



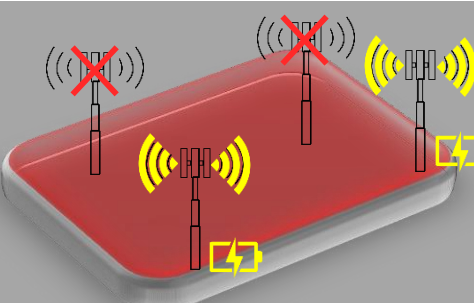
All antennas working
Full coverage
Full bandwidth

Crisis



Limited amount of antennas
Reduced coverage
Reduced bandwidth

Resilience

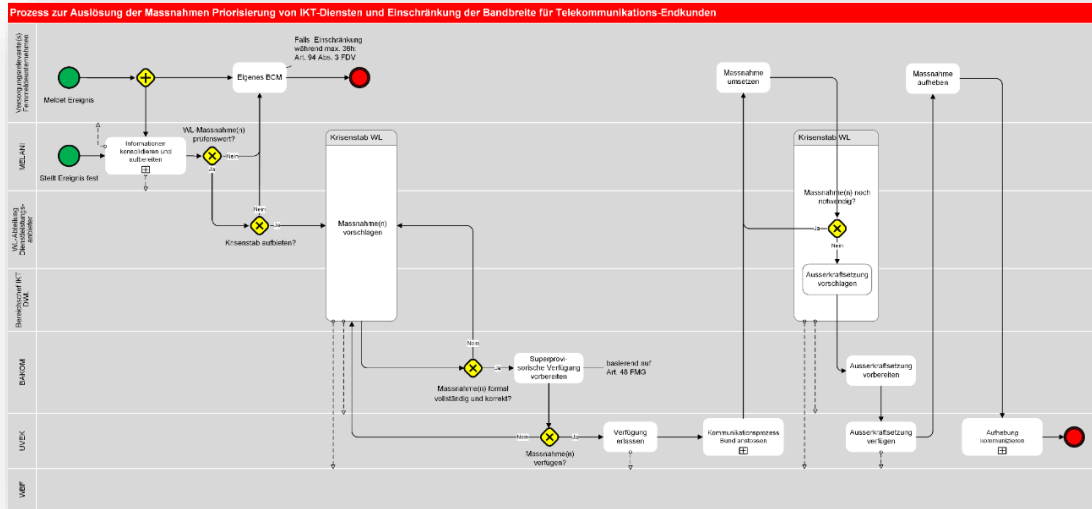


Limited amount of antennas
Resilient power supply
Increased signal strength
Full coverage
Reduced bandwidth

- Prepare for alternative network-planing
- Evaluate / Define key-infrastructure elements *with potential for increased signal strength!*
- Evaluate possible solutions for resilient power supply (i.e. Diesel generators etc.)
- Deploy resilient power supply to key-antennas
- Define processes and prepare execution with ISPs to increase signal strength including alternative network balancing
- If necessary: Combine with other measures, i.e. priority-scheme



Reactive Measures to secure the Internet



- Sometimes, prevention is just not enough
- Time is crucial
- «Better safe than sorry»
- Switzerland has established a fully defined process between various state actors and major ISPs
- Adequate Measures for different scenarios are prepared and tested
- Example: Temporary suspension of net neutrality in case of a DDOS-Attack

Questions & Remarks



Swiss Confederation
Federal Office for National Economic Supply FONES

Bernastrasse 28
3003 Bern
Switzerland





Whois



Swiss Confederation
Federal Office for National Economic Supply FONES

Bernastrasse 28
CH-3003 Bern
Switzerland

Daniel Caduff
Deputy Head of Secretariat ICT Division

