European CIIP Newsletter

November 16 - February 17, Volume 10, Number 3

Industrial Control System (ICS) Security Focus

ECN

Contents

> About ECN
ECN is coordinated with
The European Commission, was initiated by Dr. Andrea Servida,
today funded by the European Commission
FP 7 CIP Research Net CIPRNet Project
under contract, Ares(2013) 237254

>For ECN registration ECN registration & de-registration:
www.ciip-newsletter.org

>Articles to be published can be submitted to:
editor@ciip-newsletter.org

>Questions to the editors about articles can be sent to:
editor@ciip-newsletter.org

>General comments are directed to:
info@ciip-newsletter.org

>Download site for specific issues:
www.ciprnet.eu

>Founders and Editors
Eyal Adar, Founder and CEO, WCK www.wck-grc.com
Christina Alcaraz, University of Malaga, alcaraz@lcc.uma.es
Bernhard M. Hämmerli, HTA, Initiator and Main Editor bmhaemmerli@acris.ch
Eric Luiijf, TNO, eric.luiijf@tno.nl
Erich Rome, Fraunhofer, erich.rome@iais.fraunhofer.de

>Country specific Editors
For France: Michel Riguidel, ENST, riguidel@enst.fr
For Spain: Javier Lopez, UMA, jlm@lcc.uma.es
For Finland: Hannu Kari, HUT, kari@tcs.hut.fi
to be added, please report your interest

> Spelling:
British English is used except for US contributions

Cyber security landscape, challenges, initiatives and solutions

Approaching next level of security by securing against APT and introducing new concepts for securing Industrial Control System

Nowadays, cyber security should be considered as a crucial aspect of critical infrastructure protection. Networked mission critical systems and national critical infrastructure may be vulnerable to cyber threats, cybercrime and cyber terrorism. The same hazards apply to citizens and small-scale ICT systems (e.g. used by SMEs).

Currently, there are many initiatives and projects working on critical infrastructure protection and cyber security. In this issue of ECN, several European and national research initiatives focused on increasing resilience and cyber protection of CI are described. A special focus is on state-of-the art research in Industrial Control Systems (ICS), because of little computing resources and real time availability the hardest IT infrastructure to protect and to detect malware.

The EU CIPS project FACIES targets to illustrate the feasibility of a distributed approach to detect in an early stage failures and malicious adverse events of different nature in CIs.

The idea of the SAWSOC is to bring a significant step forward in the convergence of cyber and physical security technologies. SAWSOC platform is validated and demonstrated using three CI-related use-cases: air-traffic control system, energy production and distribution system, and security of mass-crowded events (at the stadium).

The EU project SEGRID's main objective is to enhance the protection of smart grids against cyber-attacks, by determining gaps in current technologies and standards through a risk management approach.

European project SECURED funded by the FP7 Programme of the European Commission, focuses on the development of a complex security framework designed to manage all user security controls at the network edge.

The increased severity and variability in extreme weather events create effects of climate change: INTACT provides methods to re-assess climate-related risk for critical infrastructure owners and operators.

VITEX 2016 is an international table-top exercise with an innovative design for CIP within the EU.

The human factor is often neglected when planning and assessing critical infrastructure preparedness and resilience. A truthful consideration.

The Criminal Use of Information Hiding Initiative launched in cooperation with Europol's *European Cybercrime Centre* (EC3) combines expertise and experience from academia, industry, law enforcement agencies and institutions to tackle the increased utilisation of information hiding techniques and prevent its wider diffusion.

The goal of the SEZBC project is to create a Cyberspace Security Threats Evaluation System (SEZBC) for national security management in Poland. With its unique and novel approach, SEZBC integrates information from monitoring of cyberspace in a country.

The Polish national project BIPSE proposed and developed CI Security System that able to ensure secure IP-communications within the power grid management network in order to response current threats to SCADA systems.

Selected projects and experiences of the NASK/Polish CERT related to threat intelligence and actionable information sharing to fight Internet threats are described.

CIPRNet Trainer is designed as an al hazard tool to exercise crises management. A report of the first industry-research training.

Some of these challenging topics were addressed during the **11th edition of the CRITIS conference** in October in Paris. see: www.critis2016.org.

Enjoy reading this issue of ECN!

Michał Choraś [1]

he holds the professor position at University of Science and Technology (UTP) where he is the Head of ZST Division. He also works as the consultant in security and coordinates projects (e.g. FP7 CAMINO on cyber crime and cyber terrorism). He is the author of over 160 publications.
e-mail: **chorasm@utp.edu.pl**

Rafał Kozik

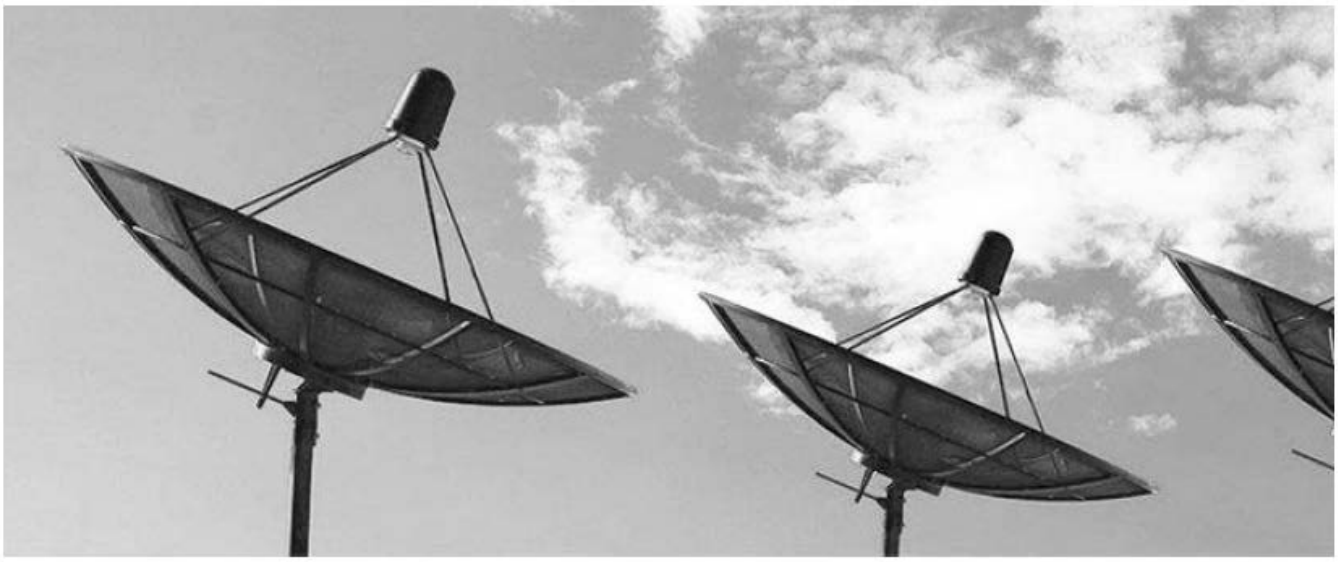
He is an assistant professor University of Science and Technology (UTP). In 2013 he received his Ph.D. in telecommunications. Since 2009 he has been involved in number of international and national research projects related to cyber security, critical infrastructure protection and data privacy
e-mail: **rkozik@utp.edu.pl**

Bernhard M. Hämmerli

Is CEO of ACRIS GmbH and Chair of ICT Security Activities at Swiss Academy of Engineering Sciences

e-mail: **bmhaemmerli@acris.ch**

He is ECN Editor in Chief



IFIP 2017 - International Conference on Critical Infrastructure Protection

The Eleventh Annual IFIP WG 11.10 International Conference on Critical Infrastructure Protection will take place in **Arlington (Virginia, USA) on March 13th-15th, 2017**.

The conference will provide a forum for presenting original unpublished research results and innovative ideas in the field of critical infrastructure protection.

Papers are solicited in the following areas of the critical infrastructure protection domain:

- Infrastructure vulnerabilities, threats and risks
- Security challenges, solutions and implementation issues
- Infrastructure sector interdependencies and security implications
- Risk analysis, risk assessment and impact assessment methodologies
- Modeling and simulation of critical infrastructure
- Legal, economic and policy issues related to critical infrastructure protection
- Secure information sharing
- Infrastructure protection case studies
- Distributed control systems/SCADA security
- Telecommunications network security

The deadline for paper submissions is **January 10th, 2016**; notification of acceptance will be communicated by February 3rd 2016. A selection of papers from the conference will be published in an edited volume – the eleventh in the series entitled ***Critical Infrastructure Protection*** (Springer) – in the fall of 2017.

For further information on the event please proceed to the following link

www.ifip1110.org/Conferences

Cyber-Physical attack analysis against Industrial Control Systems

A cyber-physical testbed, developed within the EU Project FACIES, has been exploited to study the interactions between the cyber and physical domains that arise due to physical faults and cyber-attacks against different components of an Industrial Control System.

Industrial Control Systems' (ICS) security has become a harder challenge since the fusion of ICS with Information Technology (IT) networks, as new and often unpredictable vulnerabilities and attack vectors typical from the cyber domain have emerged.

Several studies have demonstrated that the implementation of well-known cyber solutions and protection schemes is not enough, not even suitable most of the times, for ICS. In addition, as ICS generally constitute the core of Critical Infrastructures (CI), their correct, reliable, secure and safe operation is paramount. Consequently, tests can be hardly performed on real infrastructures.

With this premise, it becomes essential to develop realistic emulated environments where the analysis of the effects of cyber events on the operative conditions of the physical system can be properly addressed.

Although similar to and enhanced by standard Information Technology systems, Industrial Control Systems present unique security challenges, especially in safety-critical contexts, and generally constitute a susceptible target for malicious attacks.

The physical and cyber domains are to be studied as an overall system, considering their interactions and interdependencies, which are too often neglected.

The EU Project FACIES

In 2011, the CIPS European Project FACIES (online identification of Failure and Attack on interdependent Critical InfrastructurES) was born with the objective of illustrating the feasibility of a distributed approach able to detect in an early stage failures and malicious adverse events of different nature, taking place against CI.

Within this framework, a cyber-physical testbed has been created, where a wide number of experiments have been carried out to demonstrate and analyse the impact of cyber-attacks on the various elements of the system. These experiments include amongst others the control system, the SCADA (Supervisory Control And Data Acquisition) system, and the Fault Detection module.

The FACIES Testbed

The cyber-physical testbed consists in an emulator of a water supply and distribution system of a small city, a scaled down version reproducing a typical daily operation. For its realisation, all the main components of a real water system have been considered, from the plant (pumps, valves, tanks, pipes...) to the SCADA and control systems (Programmable Logic Controllers (PLCs), switches, Human-Machine Interfaces (HMIs)...) and (communication) networks.

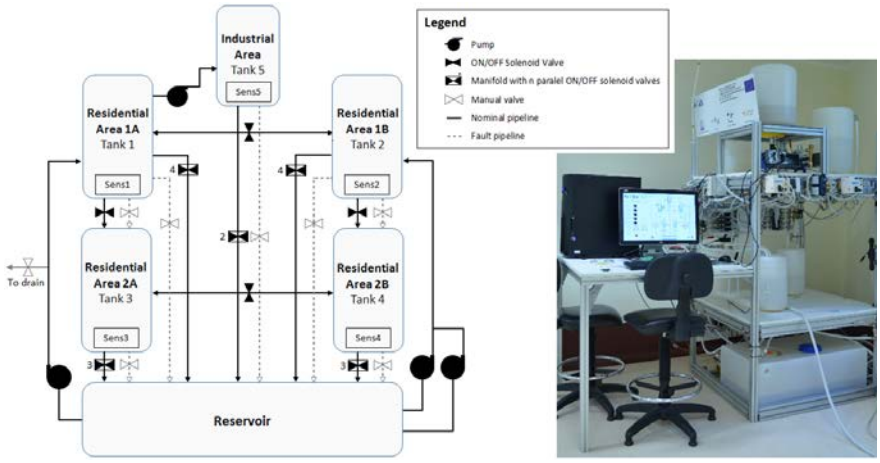
Three different areas have been considered, characterised by different water demand patterns from the customers, evolving in a six minutes scenario. The whole physical system is composed by six water tanks of different capacity, four centrifugal pumps, 20 solenoid valves, and a system of pipes.

Estefanía Etchevés Miciolino

Dr. Estefanía Etchevés Miciolino received the PhD in Engineering from University Campus Bio-Medico of Rome in 2016, where is member of the Complex Systems & Security (COSERITY) Lab since 2011. She has been involved in several EU Projects for Critical Infrastructure Protection, and received the 2014 CIPRNet Young CRITIS Award for the best conference paper.

e-mail: **e.etcheves@unicampus.it**

Eight manual valves have been included to reproduce water leaks from the tanks or along the pipes.
The system configuration allows its deployment in a large number of



different configurations (serial, parallel, crossed-connections, and their combinations). Thereby, different scenarios can be studied with high flexibility, varying from 14 nominal configurations, discretely modulating the water output flow of the tanks, and exploiting 39 different physical faults that can be induced in the testbed.

On the control side, a commercial framework has been employed, a centralised architecture consisting of two PLCs collecting the sensors measurements and controlling the actuators, deploying the Modbus/TCP for communication. Through a local TCP network, the PLCs, SCADA, HMIs and monitoring systems have been connected.

The Fault Detection System

The Fault Detection (FD) module monitors the operation of the physical system, comparing the sensors' near real-time measurements obtained from the SCADA system with the relative expected values calculated from a nonlinear model of the system, and triggers an alarm where a considerable deviation is observed, revealing the occurrence of a fault.

A graphical interface allows the operator to monitor the evolution of both the water level in the tanks and the error signal. The detected faults trigger the proper alarms on the SCADA HMI.

A wide number of experiments tested the FD's validity and effectiveness, considering both single and multiple physical faults on the system.

Testbed's Cyber Domain

Significant differences can be enumerated between ICS/SCADA systems and traditional IT networks. For the former, among others, the principal concerns and challenges are represented by the unavailability of critical data or assets, and the violation of their integrity.

Atypical and unexpected situations could be induced on the system through targeted and well-designed cyber-attacks. Assuming an attacker has already gained access to the control network, several attacks against the availability (Denial of Service (DoS)) and the integrity (Man-In-The-Middle (MITM)) of the system have been carried out. These attacks differed on the pursued goal, depending on the target component (PLCs, FD system, SCADA/HMI…), and varying from single to concurrent and/or coordinated attacks.

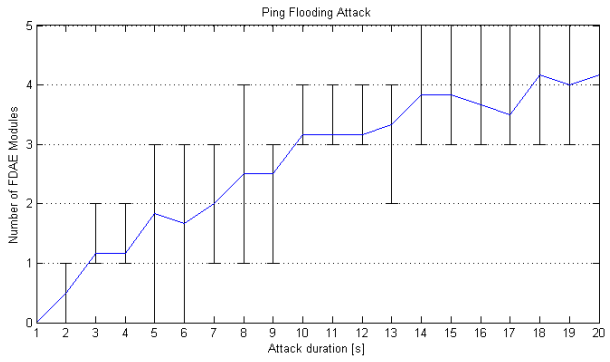
Cyber and Physical Domains Interaction

The experimental results have shown not only the FD system's validity against induced physical faults and the effectiveness of the cyber-attacks targeting the control and/or SCADA system. It was also demonstrated in *Etcheves et. al*[1] that, if the attacker gains sufficient knowledge about the system and its operation, it would be possible to cover the effects of the attacks by designing the proper combination of events and relative duration, making it hard for the operator to distinguish whether the system is undergoing a cyber or a physical anomaly.
Indeed, a complex behaviour could be obtained by combining attacks. Fake healthy information could be sent to the HMIs, while actually corrupting the system's component in a way to move it to an unstable state. The hazard is made undetectable to the operator, who is therefore not able to perform required recovery actions. Conversely, the malicious agent would be prone to emulate an attack taking place on the target system. In such a case, the operator would face the anomalous behaviour, performing recovery operations which are not actually required or, in the worst case, halting the system, moving it to an unexpected or unstable state.

If you would like to know more about FACIES please visit our website: http://facies.dia.uniroma3.it/

[1]Etcheves M. E., Bernieri G., Pascucci F., Setola R. *Communications Network Analysis in a SCADA System Testbed Under Cyber-Attacks*. 23rd Telecommunications forum TELFOR 2015, 24-25th November 2015, Serbia (Belgrade). (2015)

The FACIES Project was supported by the Prevention, Preparedness and Consequence Management of Terrorism and other Security-related Risks Programme European Commission – Directorate – General Home Affairs (HOME/2011/CIPS/AG/4000002115).



SAWSOC: An integrated platform for achieving the convergence of physical and cyber security technologies

The FP7-SECURITY Programme project SAWSOC provides an advanced security solution for enhancing Critical Infrastructure protection guaranteeing the protection of citizens and assets.

Despite logical and physical security depend on each other, it is surprising that until now many companies still treat them as separate entities. Today, technologies for implementing security in the aforementioned domains are both stable and mature, but they have been developed independently of each other. over time some advancements have been achieved – e.g. Security Event Management (SEM) and Security Information Management (SIM) have merged into Security Information and Event Management (SIEM), and Logical Access Control Systems (LACS) and Physical Access Control Systems (PACS) have merged into Identity Management (IM) – but the real convergence is still a faraway target.

The main goal of **S**ituation **AW**are **S**ecurity **O**perations **C**enter SAWSOC project is bringing a significant step forward in the convergence of cyber and physical security technologies. By "convergence" we mean an effective cooperation (i.e. coordinated and results-oriented effort to work together) among previously disjointed functions. The project provides a security platform which is experimentally evaluated in the domains of three use cases that deal with: the protection of a Critical Infrastructure for Air Traffic Management, the protection of a Critical Infrastructure for Energy Production and Distribution, and the protection of a public place, specifically a stadium, during a public event. These use cases are characterised by very different requirements and directly involve people, and thus provide concrete evidence of the improved security on the citizens.

SAWSOC idea

The basic idea behind SAWSOC is shown in Figure 1 where the most relevant security technologies are grouped in two partially overlapping categories, namely Physical and Logical. The figure emphasizes that, especially in the recent years, some solutions have been combined (i.e. SEM and SIM have merged into SIEM) but much is yet to be done.

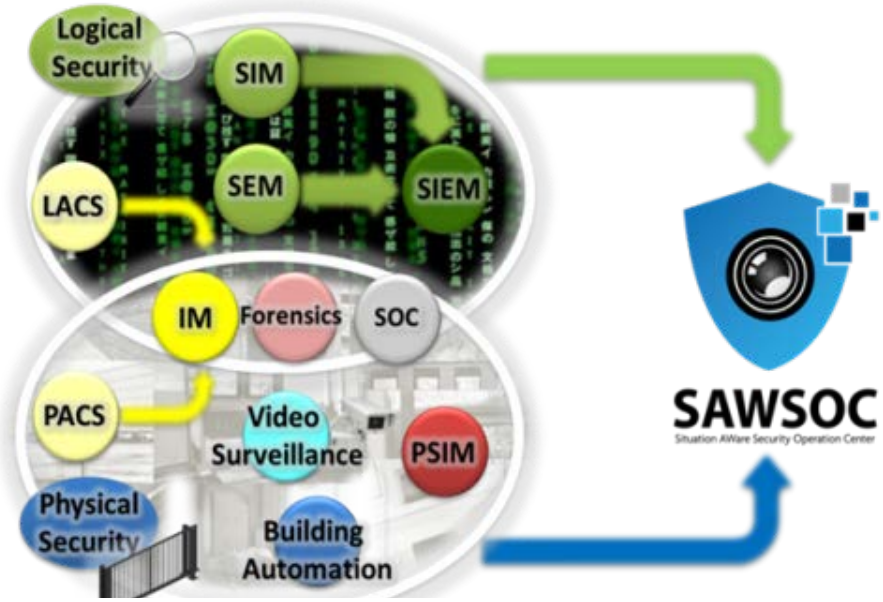


Figure 1– SAWSOC: A leap forward in convergence direction

Gaetano Papale [1]

Gaetano Papale is a PhD Student at University of Naples "Parthenope". His research activities are focused on intrusion detection, fraud detection and big data analytics. Currently, he is involved in the FP7 LeanBigData project.

gaetano.papale@uniparthenope.it

Gianfranco Cerullo

Gianfranco Cerullo is a PhD student at University of Naples "Parthenope". His field of interest is the cyber-physical security through the use of the Data Fusion techniques.

Bruno Ragucci

Bruno Ragucci has received from University of Naples "Federico II" a master degree in Computer Engineering. His thesis work was focused on Critical Infrastructure protection.

Also, Security Operations Center (SOC) technology has improved significantly, but SOC solutions have typically designed using custom specific needs. Others key security systems like Video Surveillance, Forensic support and Building automation are still a limited capability of performing complex correlations on security relevant data. SAWSOC holistic approach and enhanced awareness technology allow dependable detection and diagnosis of attacks. By "dependable" we mean:

Accurate
The detection and false positives rate must be an improvement of current State of the Art products. Accuracy is achieved by performing sophisticated correlations on multiple streams of diverse events which are collected in the logical and physical domains. It is important remarking that in contexts as Critical Infrastructures or crowded places, false alarms can be as harmful as false negatives.

Timely
It represents a challenging task, since the large amount of heterogeneous data that the system has to process in near real-time. To this end, SAWSOC platform implements the best solutions available in the field of Complex Event Processing, distributed real-time computation, and message brokering.

Trustworthy
SAWSOC is designed and implemented using fault-and intrusion-tolerant techniques. It is resilient to faults and attacks and is able to perform its tasks even in the presence of attacks or/and if itself is under attack.

SAWSOC features

The main features of SAWSOC platform are the following:

1. Enhanced situation awareness
2. Real-time monitoring facilities, implemented as dependable functions
3. Distributed platform, designed as a resilient system
4. Ability to handle data heterogeneity
5. Ability to interoperate with existing technologies
6. Ability of escalating from fault/intrusion symptoms to the adjudged cause of the fault/intrusion, and of estimating the damage to individual system components

SAWSOC use cases

SAWSOC is designed and validated considering the following use cases:

1. Maintenance Impacts and Attack Recognition on Critical Infrastructure (MIARCI)
2. Energy Production and Distribution Critical Infrastructure (EPDCI)
3. Crowded Events Safety & Security (CES&S)

The MIARCI use case is provided by ENAV S.p.A. ENAV is responsible of the Air Traffic Control (ATC) service in the Italian sky area and national airports. ENAV Security Operation Center monitors and manages several types of security events collected by a plethora of physical and logical devices including SIEM, Network and Service Monitoring Systems and Physical Access Control Systems with real-time data processing features. In this use case, the SAWSOC platform is used to protect the ATC infrastructure from malicious internal attacks (i.e. those perpetrated by company employees). SAWSOC enhanced data integration and data correlation capabilities will allow a timelier and accurate detection and diagnosis of attacks. Also, the SAWSOC awareness technology will consent to understand whether an outage is due to a legitimate maintenance operation or is the effect of a malicious attack.

The EPDCI use case is provided by the Israel Electric Corporation (IEC). IEC generates and distributes the electricity to the whole country. IEC ensures a continuous supply of electricity (only two hours per year of outage is allowed) leveraging capability to remotely control the electric grid through a SCADA system. This system includes operation centre functions, communication infrastructure and field equipment, such as: SIEM, IP cameras, biometric fingerprint readers and Intrusion Detection Systems (IDs). Under normal operating conditions, the use of this SCADA system provides continuous service guaranteeing the compliance with the Service Level Agreement (SLA). However, a cyber-attack or improper actions on the SCADA system may result in severe interruptions in the supply of the electric service. A cyber-attack can violate both security and electrical equipment by causing the sensors to show wrong information and producing damage and/or prolonged interruptions. The SAWSOC solution provides an effective coordination of the security systems and allows to backtrack he origin of the attack, the identification of the suspected person performing the attack and re-enabling of compromised sensors.

The CES&S use case is provided by Comarch S.A. and deals with the protection of a public place during an event. Comarch is the majority shareholder of Cracovia sports club, the oldest football club in Poland. Specifically, Comarch is the owner of the Krakow Stadium and must provide the citizens protection during the crowded football matches. The system used to guarantee the security of supporters is composed of CCTV cameras and biometric systems like face recognition and fan card (i.e. a magnetic card which contains all the details to identify the supporter). SAWSOC platform demonstrates the benefits of converged physical and logical security to the large public and it guarantees/supervises:

- the recognition of unusual activity taking place inside the stadium (movement of large crowd, gathering of a large number of people or people suddenly running away)
- the recognition of persons involved in some unethical or criminal activity inside the stadium
- the access to the stadium only to the authorised people

SAWSOC architecture

SAWSOC is the integrated technology platform that allows for accurate, timely and trustworthy detection and diagnosis of security attacks, combining information from physical and logical event sources. The overall architecture of SAWSOC platform is been designed through a collaborative process, during which both general and use case specific requirements have been taken into account. In Figure 2 the overall SAWSOC architecture is shown. SAWSOC platform has the ability to combine event information from multiple event sources to make sophisticated diagnosis based on the received events. It is made up of the following components:

- Video Content Analysis
- Correlation Engine
- Rule Engine
- Forensic Module
- Identity & Credential Management System
- Visualisation Module

The VCA (Video Content Analysis) receives the inputs from Video Surveillance system and focus them into high-level concepts and events. Computer vision algorithms are applied to the video streams to perform person detection, position and movement direction of the detected person, and specific action.

The Correlation Engine is the component in charge of the event diagnosis process. The attack diagnosis process is driven by correlation rules that aggregates the parameters of attack symptoms, such as the attack type, the target component and the temporal proximity. The Correlation Engine operates by correlating a huge amount of security relevant information (coming from logical and physical sources and VCA) in real-time, and implements Complex Event Processing (CEP) techniques and stream processing computing technologies.

The Rule Engine provides the logical rules followed by the Correlation Engine. It includes two main components: Signature Based Support and Anomaly Based Support. The basic concept is that the rule defined in the Signature Based Support are not enough to detect all the attempts aimed to mine overall security. The Anomaly Based Support cooperates and complements the Signature Based Support in order to detect all possible breaches to system. The Anomaly Based module operates the following two steps:

- Get events to create behaviour model
- Process incoming events passing them to the behaviour model

The output produced by Anomaly Based Support (i.e. the timestamp of involved events and their anomaly level parameters) are provided to the Correlation Engine for the decision task.

The Forensic Module provides a set of services that enable the SOC operator to trace from an event to the log data that identify it. The module ensures that the events and their associated logs are stored in a relational database, namely the Forensic Storage, for further processing and investigations.

The Identity & Credential Management System provides credentials for user authentication, device authentication, and event signing in the SAWSOC platform. This information is used, for example, to allow a trusted employee to enter in a secure location or access to a secure IT system, or to allow a trusted device the connection to a secure network.

The Visualisation Module is a powerful Human Machine Interface able to present to the user the alerts received from the Correlation Engine. It has been developed in such a way that the user has an immediate understanding of the situation in order to take proper and quick actions. This component provides also functionality for forensic evidence, such as browsing logs of original events and generating reports.

SAWSOC Demonstration

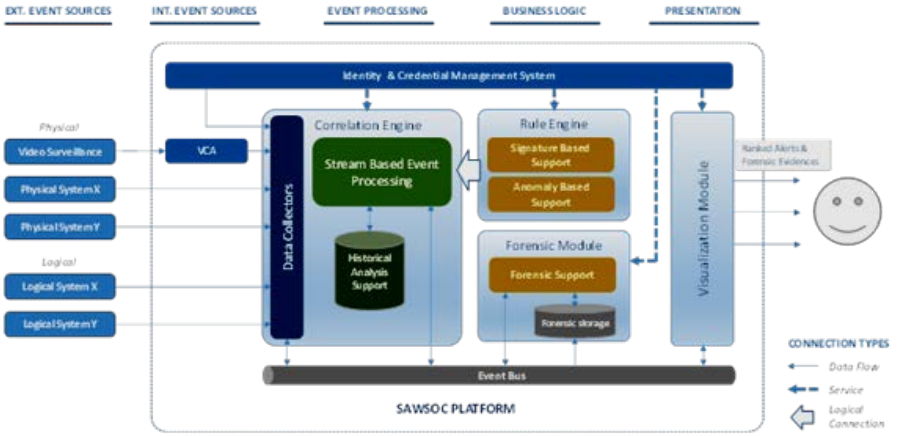


Figure 2 – SAWSOC Platform: Overall Architecture

In the following the features of SAWSOC platform are demonstrated.

In order to present misuse-based detection, effectiveness of Visualisation module, event correlation and data fusion features, the CES&S use case has been considered as a reference scenario. This demonstration consists of a detection of a guard during his/her patrol path.

Each sector of the Krakow Stadium is controlled by means of a camera (whose output is analysed by the VCA module) and by using Bluetooth beacons. VCA and Beacons are used to identify the guard during its patrolling. Three situations may occur: In the first case both VCA and Beacon recognise the guard. This case is a no alarm situation and the Visualisation module lights the corresponding sector of the stadium green.

The second case occurs when the guard is detected only by either the VCA or a Beacon (the order is irrelevant). This case is a warning situation and the sector turns orange.

Figure 3 – An alarm showed by Visualisation module

The last scenario occurs when the guard is not detected both by VCA and Beacon. This is the alarm situation and the colour of the sector turns red (sector B4 in Figure 3).

In addition to these situations, the SAWSOC platform is able to detect many other events and it is customizable according to the user needs. For example, SAWSOC detects an alert also if the guard takes too much time to pass a sector or to complete the entire patrolling path.

The SAWSOC cyber-physical security provisioning features are demonstrating in the EPDCI use case. Suppose that the network administrator of a Power Grid company is corrupt or he/she has been bribed to install a proxy machine implementing a Man-in-the-Middle attack. The goal of the attack is to disrupt supplying power to a big number of customers and hide from operators the real state of the system. The attack sequence consists of the following steps:

1. A person enters the secured room using his personal badge and is then detected by the camera. This event does not generate an alarm situation

2. If the person unplugs one of the Ethernet cords from the rack and connects a new device, these events are detected as a warning (Figure 4)
3. The attacker connects his device and performs the attack (taking the control of one or more Remote Terminal Unit and blind the control to the entire SCADA system). This event is detected as a warning.

Figure 4 -Detection of router state change – Warning situation

Now, the SAWSOC Correlation Engine correlates all these events, detects the malicious pattern and generates the alarm. In Figure 5 is depicted the visualization of an alert situation in case of Man in the Middle attack detection. The Visualization module shows the equipment that has generated the alarm and its location within the infrastructure.

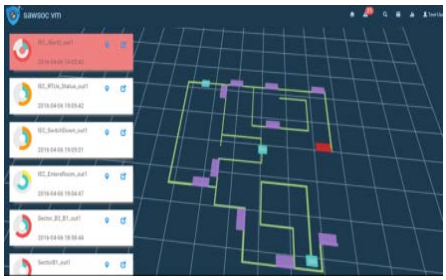


Figure 5 – Man in the Middle attack detection

The SAWSOC platform anomaly based capability is demonstrated considering the MIARCI use case. ENAV security policies provide that within the ATC (Air Traffic Control) room two operators must be simultaneously present at every desk. In case of one operator is not present, the post should not be activated. Each operator has at his position: a headset, a monitor that shows radar information and an authentication pad to log in. We consider an internal attack in which an operator has stolen the credentials of his colleague. Now, he can access to ATC room, sits to his position and logs in to it. After a while the attacker can move to his twin post and logs in with the stolen credentials of the unaware colleague. In this way, a single operator can take control of ATC position and perpetrates malicious actions. The SAWSOC platform detects the insider attack thanks to the inconsistency between the Physical Access Control system of the room and Logical Access Control at the post, specifically:

- One person enters the room, whereas two operators are logged in
- The legitimate owner of stolen credentials is not in the room, but is logged at the post
- VCA counts one person at the desk, but two employees are operating

SAWSOC platform focused all these events and triggers an alert (Figure 6).

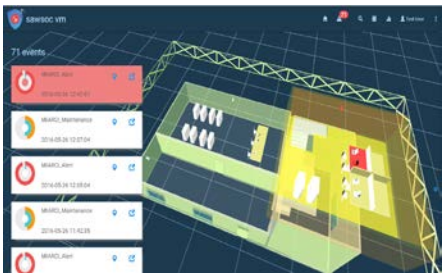


Figure 6 – Insider attack detection

The SAWSOC Consortium

The SAWSOC Consortium consists of 11 partners: Selex ES S.p.A. (Italy), CINI - Consorzio Interuniversitario Nazionale Per L'Informatica (Italy), Fraunhofer-Gesellschaft zur Foerderung der angewandten Forschung e.v. (Germany), The Israel Electric Corporation Ltd (Israel), ENAV S.p.A. (Italy), Intercede Ltd (United Kingdom), Espion Ltd (Ireland), Lonix OY (Finland), Bergische Universitaet Wuppertal (Germany), Esaproject SP Z OO (Poland) and Comarch S.A. (Poland).

Security for Smart Electricity GRIDs

SEGRID's main objective is to enhance the protection of smart grids against cyber-attacks, by determining gaps in current technologies and standards through a risk management approach, and by developing and testing novel security measures for smart grids.

The SEGRID project, funded by the EU under the FP7 program is a three-year (2014-2017) collaborative project coordinated by TNO.

SEGRID use cases

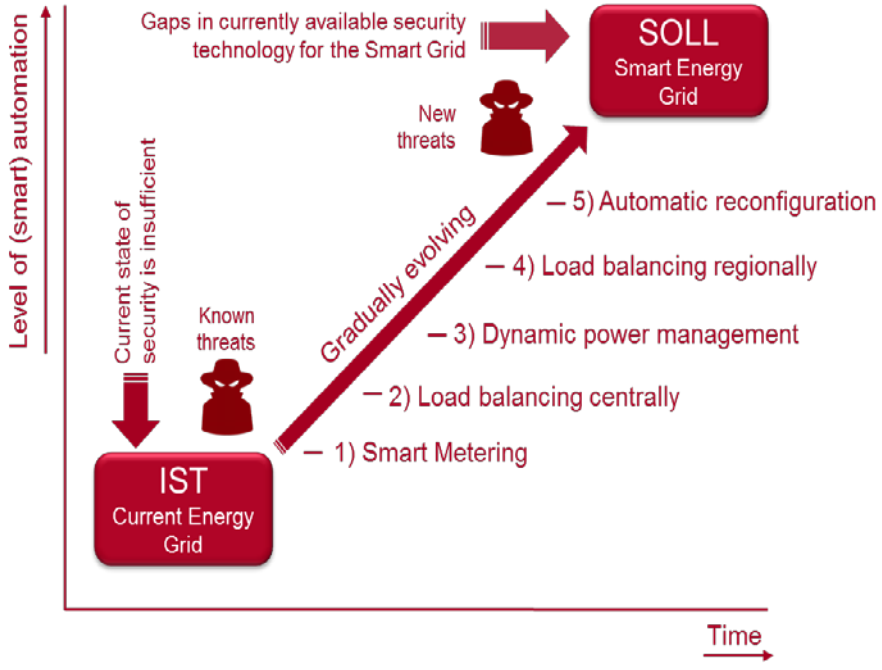
A smart grid can be considered as a utility-wide system (-of-systems) that will of course not come into being overnight, so it will be composed of a mix of old and new components. This is why SEGRID introduced the concept of a gradually evolving system in which new functionality is added to accommodate new use cases. We have deduced five use cases (The SEGRID use cases) that clearly demonstrate this gradual evolving systems concept (figure 1).

The SEGRID use cases have been selected based on the work already done by ENISA along with the working parties involved in the mandates 441 and 490, as well as based on the work and competence of the project partners. The rationale for the SEGRID use cases is based on:

- Relevance for new business, economic growth, and supporting the introduction of more sustainable and locally generated power;
- Addition of new functionality and components that inherently will introduce new vulnerabilities and a wider cyber-attack surface.

The SEGRID use cases cover the most relevant security issues that will arise from the increasing complexity of smart grids, which is confirmed by the strategic plans of the SEGRID Distributed System Operator partners Alliander and EDP.

Figure 1 : The SEGRID storyline and use cases



Reinder Wolthuis

Reinder Wolthuis, M. Sc. is senior project manager and consultant cyber security at TNO (since 2006). He has almost 20 years of experience in innovation in information- and cyber-security. He participated in and led many security projects, involving innovations in (cyber)security, conducting security benchmarks & assessments, and security consulting
Reinder is the coordinator of the SEGRID project, leads WP6 (dissemination), and is involved in the risk assessment work of WP2.

e-mail: **reinder.wolthuis@tno.nl**
TNO
Eemsgolaan 3
9727 DW Groningen
The Netherlands

SEGRID objectives

The objectives of the SEGRID project are:

1. Establish security goals and determine threats of the SEGRID use cases.
2. Define the gap between available and needed security for smart grids, and develop new security methods, designs and tools to fill the identified gap.
3. Evaluate and enhance existing security risk and vulnerability assessment methodologies in order to encompass the increasing complexity of smart grid.
4. Evaluate and test new developed security methods and tools for smart grids (in realistic testbed environments), and assess their cost versus the consequences of failure.
5. Ensure that the SEGRID results are fed into the appropriate industrial partners, standardisation groups, governmental bodies, research community and regulators and to raise awareness

The supervision and automation of power infrastructures is extending from the SCADA (Supervisory, Control, And Data Acquisition) control rooms to the high- and medium voltage network operations, and even low voltage networks, through monitoring and control of household appliances and renewable energy sources. This concept is generally referred to as the 'smart grid'. A smart grid essentially encompasses the smart automation of the complete transmission and distribution infrastructure that is needed for electric power transport; it covers the complete energy conversion chain from (distributed) generation to consumer.

First project results

SEGRID currently is in its third year and the first results are ready. We have detailed our SEGRID use cases, where each use case was split into several scenarios. We have selected a suitable risk assessment (RA) approach from several industry standard RA approaches and conducted a detailed RA on a number of the scenarios. These provide, combined with the smart grid security and privacy goals that were drawn up, valuable input for the development of new security measures. We also are working on enhancement of the risk assessment methodology, which includes aspects such as threat actor capability and motivation, societal impact, and dependencies between systems and stakeholders.

We are also working on enhancing and automating vulnerability assessment, where we use KTH's Cyber Security Modelling Language (CySeMoL) as a basis.

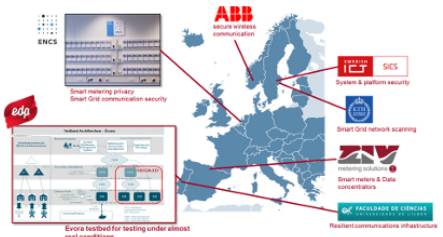


Figure 2: SEGRID Integrated Test Environment (SITE)

We have designed the SEGRID Security & privacy architecture (SPADE), a general design process to define security and privacy architectures specific for single use cases. Some of the concrete new security measures that SEGRID is working on are:

- Trusted platform, improvements to platform security solutions for devices in the smart grid.
- Resilient SCADA systems, to make the SCADA system tolerant not only to accidental failures but also intrusions.
- Enhancing IDS in mesh networks, by network traffic analysis and through authentication.
- resilient communication infrastructure for the core WAN network of a smart grid, by applying Software Defined Network (SDN) principles.
- Robust and scalable (D)TLS-based communication by improving its robustness and tolerance to Denial of Service attacks and key material provisioning during the (D)TLS handshake process
- Key management for group software distribution to distribute, revoke and redistribute (i.e. rekeying) the security material currently used within the group,
- Privacy-by-design solutions for the SEGRID Use Cases, by collecting and creating new privacy design patterns and Privacy Enhancing Technologies

To test these solutions, we have implemented the SEGRID Integrated Test Environment (SITE, see figure 2), which is a distributed test environment.

SEGRID Consortium

The SEGRID Consortium consists of ten members from five different countries. The consortium represents a well-balanced and strong partnership among DSOs, manufacturers, universities and research institutions,

The ten partners in SEGRID are:

- Organisatie voor toegepast natuurwetenschappelijk onderzoek TNO (NL)
- Swedish Institute of Computer Science (SE)
- Kungliga Tekniska högskolan (SE)
- Instituto Consultivo para el Desarrollo (ES)
- European Network for Cyber Security (NL)
- Liander NV (NL)
- ABB AS corporate research (NO)
- Foundation of the Faculty of Sciences of Lisbon University (PT)
- Energias de Portugal (PT)
- ZIV Metering Solutions S.L. (ES)

If you would like to know more about SEGRID please visit our website: www.segrid.eu

SEGRID has received funding from the European Union's Seventh Programme for research, technological development and demonstration under grant agreement No. 607109.

Promoting user-centric security in cyberspace: SECURED - SECURity at the network Edge

The growth of the Internet in recent years has transformed the way in which we manage business operations, engage in day to day activities, and communicate both personally and professionally, making it an indispensable pillar of modern society. With the advent of smart technologies, particularly within the framework of the Internet of Things (IoT), individuals have come to rely on a range of connected devices in the home and office environments. Depending on their role, individuals may not only be responsible for the security of their gadgets, but also those of their children or employees. At the same time, threats in cyberspace, such as malware, are on the rise, and even the most vigilant users are susceptible to a range of cyberattacks.

Managing the security of multiple devices through the configuration of various security applications rarely, if ever, provides a level of uniform security capable of protecting data and personal information. Moreover, many of today's smart devices, especially those used in the home, are not capable of independently running security software, despite the fact that they are connected to the Internet in some capacity and are therefore vulnerable to attack. This new environment requires that users be effective in managing their cybersecurity needs by employing both a proactive and streamlined approach.

SECURED, a project funded by the FP7 Programme of the European Commission, focuses on the development of a complex security framework designed to manage all of a user's security controls at the network edge [1]. In simpler terms, SECURED can be perceived by end users as a portal or initial entry point allowing them access to an individualised profile through which they can manage all aspects related to the cybersecurity of their devices before connecting to the Internet. Profiles are protected in a user repository that can be accessed through the cloud or a network edge device, such as a router, and are only accessible via a secured, verified connection that is remotely attested and can be made available through a trusted third party host, for example a user's telecom provider.

Within this trusted virtual domain, users can configure their security controls. All of a user's security settings previously defined through SECURED will also become operational during this stage. Basic and expert users will have the option to manage their security requirements (policies) as they see fit, with expert users able to customise security controls through medium-level security requirements, while basic users can express their preferences via the use of checkboxes referring to easy-to-read security statements and high-level security requirements. Depending on the requirements selected, SECURED will be able to determine which personal security applications (PSAs) to automatically assign to the user, such as those developed for anti-phishing, content filtering, network monitoring, etc. User requirements are enforced at the level of a network edge device (NED), ensuring that all traffic to the user's device is checked in accordance with security requirements, and that user preferences are transportable, providing uniform protection across all devices and Internet access points. In addition, user security requirements are part of a hierarchical structure, or policy stack, that can be beneficial to employers and parents aimed at keeping their networks and dependents safe, as will be highlighted below when discussing the practical applications of SECURED.

Francesca Bosco

Unicri (United Nations Interregional Crime and Justice Research Institute)

Francesca Bosco is UNICRI Programme Officer. She is responsible for cybercrime and cyber-security related projects and member of the Advisory Groups on Internet Security Expert Group of the EC3.

Email: **bosco@unicri.it**

Arthur Brocato

Unicri (United Nations Interregional Crime and Justice Research Institute)

Arthur Brocato is a Fellow at UNICRI, working within the Emerging Crimes Unit on issues related to cyber-security, terrorist organizations' use of the Internet, and other security-related projects.

Email: **brocato@unicri.it**

[1] Further information on SECURED can be found by visiting the project's website, available at: https://www.secured-fp7.eu/

The PSAs that have already been developed by the SECURED consortium include those designed for packet filtering, application filtering, content filtering, re-encryption, anti-phishing, network monitoring, anonymisation, bandwidth control, and a corporate VPN. As more PSAs are developed and refined, users will be able to uniformly protect all of their devices with applications that are able to adapt to mitigate the risks posed by emerging cyber threats. The protection of communication channels and certain traffic stipulated by users provides a robust form of data protection.

Real World Applications

The possible applications of the SECURED technology in the real world are manifold; however, within this context, the positive effects for child online protection, businesses employing bring-your-own-device (BYOD) policies, and individual management of devices within the IoT should be highlighted.

The protection of children and minors online has continuously been an issue of critical importance for parents and policymakers alike. Offering parental controls has become fundamental for Internet service providers since the age of dial-up connections; however, with the proliferation of mobile devices, laptops, and other gadgets, parents can have a harder time enforcing security policies across a range of their children's devices, while also being assured that these policies are uniform in nature when referring to devices that utilise differing telecommunications services. By using SECURED, policies for all devices can be implemented through a single control centre, allowing parents to comprehensively restrict access to certain websites; categorically themed areas of the web, including gambling, pornography, and extremist websites; applications; and chat rooms, all of which can serve as areas of illicit activity.

As mentioned above, the hierarchical policy stack of SECURED represents a positive feature for parents, in particular, as well as for employers. In the event that policies higher up in the stack are active, users of SECURED, in this case children, would be notified of these overarching policies before accessing the Internet.

With respect to the workplace, aside from headline-catching cyberattacks against large corporations, small and medium enterprises (SMEs) are increasingly becoming targets of cybercrime. These entities represent weak links in the cybersecurity chain, having few or no IT experts employed within their organisations, while also potentially serving as backdoors for cybercriminals to enter the systems of large corporations with whom the SMEs have a business relationship. Start-ups, small family run businesses, or even larger entities may rely on employees to use their own laptops and other devices for carrying out their work, risking sensitive payment data being exposed via a single employee carrying out an unencrypted transaction.

BYOD policies may be more cost effective for employers, but the ramifications of a data breach can significantly damage the reputation and financial standing of any company. Through SECURED, businesses and other organisations can mandate that all employees accessing the Internet via their networks maintain a certain level of security on their personal devices. This ensures that anyone accessing the NED has a secure connection and uniform policies in place, before surfing the Internet.

Finally, with the expansion of the IoT, laptops, desktop computers, and smart phones will come to represent only a fraction of the devices connected to cyberspace. The refrigerator that is capable of notifying its owner via the Internet when it is low on milk, or the ability of homeowners to control their thermostats remotely are only a few examples of IoT technology currently in existence.

The IoT exists beyond the home environment, extending to the workplace and capable of connecting heavy machinery, monitoring accessories in hospitals, tracking mechanisms for transport, and other sensitive equipment across an array of different sectors. SECURED technology acts as a focal point for security management and can therefore significantly assist actors from a variety of sectors in the administration of their respective security architectures in the IoT. The system addresses the needs of devices that are more at risk: devices having limited computational power (and therefore unable to locally execute security controls) and devices that run on custom platforms, which may not be designed with security in mind. In short, administrators controlling the NED of their respective IoT networks have the ability to protect all of their connected devices of varying sophistication as they see fit, customising security controls to meet their personal or business needs, while incorporating devices that may not be able to execute cybersecurity measures via their own accord.

Conclusion

In conclusion, establishing a uniform level of cybersecurity across all user devices to defend against emerging threats has become paramount for ensuring adequate protection in cyberspace. Moreover, SECURED's use of trusted virtual domains at the network edge for setting up individualised security controls adds a much needed level of trust and verification to the configuration process and overall cyber ecosystem. Easy specification of security policies simplifies configuration and hence encourages users to take direct control of their protection. As stakeholders in the tech and international community strive to promote a global culture of cybersecurity, SECURED's user-centric architecture and approach to device security serve as valuable components for achieving this aim.

Risk management support on critical infrastructure protection against extreme weather events

The increased severity and variability in extreme weather events resulting from effects of climate change, requires critical infrastructure owners and operators to re-assess their risks: the INTACT project supports this process.

INTACT is an EU FP7 project which aims

to offer **Decision Support**

to **CI operators and policy makers**

regarding **Critical Infrastructure Protection** (CIP)

against changing **Extreme Weather Event** (EWE) risks

caused by **Climate Change**.

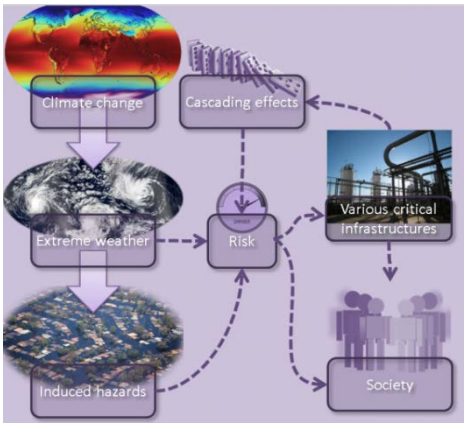
We have five case studies in which we have developed and tested our concepts with a variety of true local end-users:

- Landslides, in the Campagnia region, Italy;
- Flash floods, in the Southern region of Spain;
- Flooding the Cork area, Ireland;
- Winter storms, in the Pirkanmaa region, Finland;
- Flooding, in the Rotterdam Harbour, Netherlands;

We now have entered the final stage of the project in which we will validate our concepts with the end-users in each of the case studies.

INTACT Wiki

The main concept of the INTACT project, depicted in the figure below, is how we connect the various domains/ expertise, with risk (management) as key-point.



This concept is also depicted on the home page of the INTACT Wiki:

www.intact-wiki.eu

The INTACT Wiki is the platform in which the knowledge, tools and methods, developed in INTACT are shared with the world. On it, you can find information, references, guidance, and experiences on how to ensure continued resilience of critical infrastructures in the context of changing climate and related extreme weather events. This information is primarily directed at operators of critical infrastructures and policy makers involved with these critical infrastructures and can be used in various ways.

The Wiki contains a large amount of interconnected information that attempts to cover the needs of a wide range of potential users. In order to support users looking for a specific type of information, we provide several entry points that direct them to the various sections of the Wiki that would be of most interest to them.

In this way, the Wiki serves as a user friendly and intuitive online repository on valuable background information and knowledge about climate change, EWE, and CI, with examples, illustrations and references. Amongst other, it contains data on:

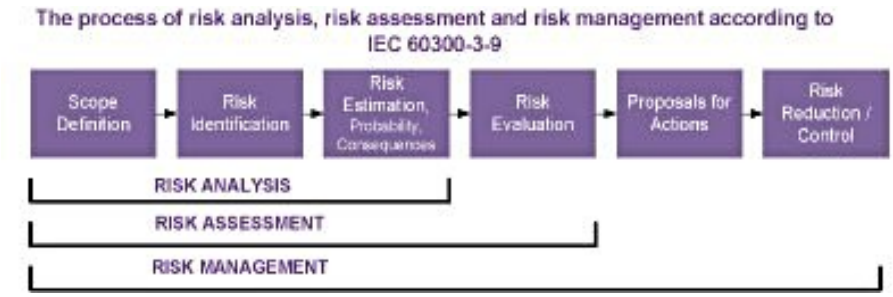
- Climate change for the medium-term & long-term period;
- Changes in frequency and strength of EWEs;
- Changes in induced hazards;
- State-of-the-Art tools and methods used in risk assessment;
- Specific vulnerabilities for EWE for specific CI;
- Assessed best practices on mitigation measures;

Peter Petiet

Peter Petiet is a senior project manager at the Netherlands Organisation for Applied Scientific Research TNO. Amongst current other activities, he is the project coordinator of the EU FP7 INTACT project.

Since 2010 he has led many projects on technical and organisational innovations within safety and crisis management domains,
and on carbon capture innovations and business-to-business projects within the oil and gas domain.
His main interest is on connecting worlds, organisations and people for the sake of business continuity, increased efficiency and effectiveness and increased safety and security.

e-mail: **peter.petiet@tno.nl**



Step-by-step method

In order to use this data to determine the future EWE risks to your CI, and to guide the user through this large information source (depending on the type of CI and EWE that are of interest to the user) we have developed a step-by-step method using the risk management process presented in BSI (2010).

The risk management process identifies the main steps comprising 'good practice' in decision-making. It recognises the circular nature of risk management, which may require the review of the risk analysis and assessment after implementation of risk reduction control measures. The steps of the process are:

- **Scope definition**

  Determines the scope of the risk assessment in terms of the CI, the information needed and the type of approach, timeframes and scales to be considered;
- **Risk identification**

  Explores and classifies the main hazards and vulnerabilities taking into account cascading effects;
- **Risk estimation:**

  Assesses the risk magnitude using available models and taking into account uncertainties;
- **Risk evaluation:**

  Assesses the magnitude of risk considering the particular context of the CI;
- **Proposals for action:**

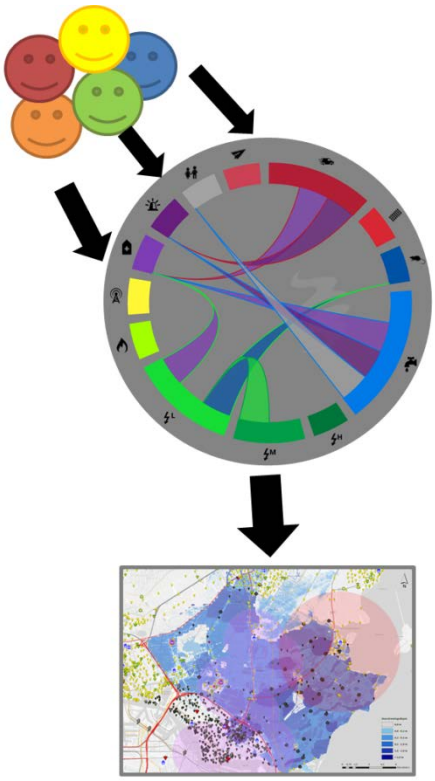
  Provides guidance on the possible mitigation measures to reduce the estimated risk;
- **Risk reduction control**

In each of these steps, it is described why which tools/methods are applicable, and how you should use them. One example tool, used in the each of the five case studies, and found very valuable for CI operators/ owners to get a notion of potential cascading effects, is the C!RCLE tool.

C!RCLE is a support tool for different network owners, stakeholders and authorities or governments to find out and discuss cascading effects together in a workshop setting. During the discussion, dependencies between the networks or objects are drawn and the causal relationships between them are collected in a database (example figure shows results from the Irish case study, Cork).

What we found is that many CI owners and policy makers already have their own risk assessment/ management methods in place. With our approach, we do not just develop another method, but we tend to support them with all mentioned valuable information.

They should still use their own familiar current tools and methods, and possibly including our data on (future) EWE, and on subsequent induced hazards.



INTACT project and consortium

The INTACT project has been launched on May 01, 2014 and will deliver its final results in 2017. TNO is coordinator of the project consortium with eleven partners from eight countries: CMCC (IT), DELTARES (NL), FAC (IRE), DRAGADOS (SP), HR Wallingford (UK), PANTEIA (NL), NGI (NO), CSIC (SP), Un Stuttgart (GE), Un Ulster (UK), VTT (FI).

In case you would like more information on the INTACT project and its outcomes, please visit our websites:

http://www.intact-project.eu

http://www.intact-wiki.eu

or mail us at info@intact-project.eu.

References & acknowledgment

BSI (2010), "Risk management. Risk assessment techniques", BS EN31010:2010

Hounjet, M.W.A., Kieftenburg, A.T.M.M., and Altamirano, M. (2015), "Learning from flood events on Critical Infrastructure: relations and consequences for life and environment (CIrcle)", Available at: https://www.deltares.nl/app/uploads/2015/04/Learning-on-flood-events-on-CIrcle.pdf [Accessed August 2016]

INTACT (2016), "Draft prototype IRG". [Online] Available at: http://www.intact-wiki.eu/ [Accessed August 2016]

Räikkönen, M., Mäki, K., Murtonen, M., Forssén, K., Tagg, A., Petiet, P.J., Nieuwenhuijs, A.H. and McCord, M. (2016), "A holistic approach for assessing impact of extreme weather on critical infrastructure", in International Journal of Safety and Security Engineering, Volume 6, Issue 2, pp 171-180

The research leading to these results has received funding from the European Union Seventh Framework Programme (FP7/2007-2013) under grant agreement n° 606799. The information and views set out in this publication are those of the author(s) and do not necessarily reflect the official opinion.

VITEX 2016 international table-top exercise

An innovative exercise design in the context of critical infrastructure protection within the EU.

Scenario

VITEX 2016 provided an intensive and innovative learning experience for participants from various disciplines and 22 Member States. The target group consisted of government specialists in the field of civil protection and electricity, and representatives of national (power) grids - internationally known as the Transport System Operators (TSOs). The table-top was based on scenario-based policy discussions, which means that the participants made use of situation descriptions to discuss the possible implications within a particular context. The main storyline was that the EU Critical Infrastructure Energy was affected. The shortage of power in Europe was a result of an extremely dry winter and a hot summer, which caused low water levels in rivers. Cooling water became scarce, ships loaded with coal could not reach the coal plants, an explosion of jellyfish clogged the pipes of cooling water and the electricity demand to power refrigerators, air conditioners and other cooling systems increased tremendously.

Security, economic stability and the general well-being of EU citizens largely depend on critical infrastructures and the services they provide. The make-up of a single country's critical infrastructure is complex, not least because of the dependencies and linkages with other countries.

All the more reason to strengthen the ties between EU Member states on this subject by facing challenges together during an exercise on different levels: international, national and public-private.

Therefore, the NCTV organised the international exercise VITEX 2016 in Amersfoort on 11 and 12 May 2016. The exercise was financed from the Internal Security Fund (ISF) of the European Commission.

Objectives

1. Bringing relevant existing networks together both at a national level, and a cross border level.

2. Strengthening the awareness of the need for cooperation for protecting Critical Infrastructure (CI).

3. Strengthening the awareness of the need for joint CI exercises (public and private).

4. Enhancing insight in the impact of the disruption or failure of CI on society, including the cascading and cross border effects.

5. Gaining insight in how cooperation can mitigate the impact of potential disruptions of CI and society.

6. Further establishing guidelines or lessons learned in a concise way.

Jeroen Mutsaers

Jeroen Mutsaers (MSc) is a policy officer at the Dutch Ministry of Security and Justice working on (inter)national security and resilience and climate change adaptation. He is the Netherlands CIP contact point and is currently involved in the novel national approach for CI and resilience.

Alyssa Brinkhof

Alyssa Brinkhof works as a project leader in the resilience department at the Dutch Ministry of Justice. Among other things, she was involved in the development, coordination and delivery of the VITEX 2016 Tabletop. Alyssa has a background in International Relations.

Innovative Exercise Design

The focus of the VITEX innovative exercise design is on interaction between the participants. To support this, the VITEX exercise design consists of scenario-based group discussions that are interlinked with several supporting elements:
1. blind spot identification;
2. lexicon development;
3. knowledge market;
4. expert feedback.

Scenario Based Group Discussions

VITEX 2016 consisted of four rounds, with each round having a different thematic focus. This served to facilitate insight in the differences and similarities in approach for the various cooperation levels that can be distinguished during a crisis of this type. The focus in the first round was national; what does this scenario mean for your own country and how are things organised? This first round was played within the setting of the national team. The focus in the second round was also national, but now countries had the opportunity to discuss differences between countries on a national level. The third round focused on cross border cooperation, while the last one focused on EU-wide cooperation.

Blind Spots

There are two different types of blind spots.

1. When collaborating cross-sector or cross-border, participants may come across things they do not know, e.g. ways of working, procedures or contact points. Beforehand, they may not have been aware that they did not know this but during discussions it became clear more knowledge was needed.

2. It is also possible that participants are aware they need more information but do not know where to find it. The focus on the collection of blind spots creates a 'safe' learning environment, in which it is alright for participants to share that they do not know something. In addition, participants can actually help others by sharing their blind spots.

Lexicon

International communication is complicated by the fact that terms and definitions may differ per country. The VITEX exercise design increases insight in terms and definitions by acknowledging this and by building a lexicon together. The Critical Infrastructure-Pedia (CIPedia) was used as a support tool. In CIPedia terms and definitions in the field of Critical Infrastructure Protection are collected and shared (www.CIPedia.eu).

Knowledge Market

The VITEX exercise design allows relevant EU projects and organisations in the field of Critical Infrastructure to present themselves at a 'knowledge market'. These EU organisations and projects are not that well known by the participants. By giving them the opportunity to meet the EU organisations, and speak to them about their tasks and possibilities the participants will understand better how they could benefit from these organisations and how they can collaborate during an incident or crisis.

Expert Feedback

The experts appreciated the elements of the innovative exercise design and participated in the discussions actively by correcting false assumptions, and giving feedback at the end of each part. Their feedback focused on elements that were missing in the discussion, specifically relating to cooperation.

Conclusions and follow up

VITEX 2016 has led to a greater awareness of the interdependencies and has both the potential and the problems of cooperation highlighted at national level and between Member States. The exercise contributes to knowledge and awareness on the European crisis management structures and reinforces the cooperation between EU Member States in protecting critical infrastructure.

Within the realm of CIP there are many networks, but a platform where public and private actors interact and explore the whole of national and international cooperation is a place that is largely unexplored. That is why the VITEX exercise was developed with a focus on building cross-sector and cross-border cooperation. The evaluation made clear that the participants appreciated the VITEX exercise and that they would like to use exercises like VITEX 2016 to explore the various levels of cooperation more often. In various cases the exercise organisation was told that even the simple fact of having to compose a national team with the required field of expertise involved, had in itself been very valuable.

Exercise Guide

Besides the evaluation of the exercise, an exercise guide with the exercise design is available, which describes step-by-step how such a meeting can be organised. This guide is available for everyone to encourage possible follow up exercises in the future.

Please contact:
vitex@nctv.minvenj.nl if you are interested in the exercise guide.

Critical Infrastructure Preparedness and Resilience – The Human Factor

We all view the world with our own lens, a factor of our experiences and perceived opportunities. Immersed in our formulae and offices it is easy to forget who benefits and who loses based on the decisions we make.

Most communities today, are dependent upon critical infrastructure (CI): without power, water, sewage treatment, gas pipelines, road and communication networks, daily life would come to a standstill. On a day-to-day basis, thousands of people are working to ensure that these systems remain operational and that society benefits from the advances in technology.

If you are one of those thousands of people, I would like to challenge some of your perceptions and improve the quality of decision-making.

What do you see?

Figure 1: Transmission line

If you answered "a high tension power transmission line system" you would technically be correct. But, there is another consideration: it is Judy's lifeline. Judy is 75 years old and is dependent upon her oxygen machine 24 hours a day, seven days a week. Without power, her oxygen machine will not function. Without oxygen, she will die.

There are millions of "Judys" in the world; people dependent on machines to keep them alive; life-saving medications that need to be refrigerated; homes that need to be kept warm; and communication channels that are need to respond to medical emergencies and crimes in progress. Millions more are dependent on CI to earn a living and support their families. Your work to enhance and protect critical infrastructure is important.

Your work doesn't just support an industry; what you do saves lives. CI can reduce suffering; save jobs and reduce financial losses; and protect the environment.

Not only does consideration need to be given on a day-to-day basis to ensure that often aging CI is functioning and able to meet the growing needs of the community, but increasingly, CI is threatened by disasters. Disasters can be caused by natural hazards (such as earthquakes or floods), diseases and epidemics (such as Avian flu or H1N1) or human-caused hazards. Human-caused hazards can be result from acts of omission (the dam wasn't built properly and collapsed) or by acts of commission (a terrorist planted a bomb in an urban centre).

> "Your work to enhance and protect critical infra-structure is important. Your work doesn't just help to support an industry; what you do saves lives."

Regardless of the cause, disasters are increasing. "There were 353 disaster events in 2015, of which 198 were natural catastrophes, the highest ever recorded in one year. There were 155 [human-caused] events."[2] There is no question that with the results of climate change becoming more visible, as we see natural hazards occurring in places where we never have seen disasters before, CI will increasingly be compromised.

Laurie D. R. Pearce

Dr. Laurie Pearce is an Associate Faculty member at Royal Roads University in Victoria and a Research Associate at the Justice Institute of British Columbia in New Westminster, both in British Columbia, Canada.

She sits on Canada's National Platform for Disaster Risk Reduction Advisory Committee and Chairs the Resilient Communities Working Group. One of her primary research interests lies in promoting investing in disaster mitigation strategies at the local community level and in increasing community disaster resilience. A current research project, the Aboriginal Disaster Resilience Project, can be accessed at https://adrp.jibc.ca

Laurie.Pearce@royalroads.ca

[2] Swiss Re Sigma. (2016). N*atural catastrophes and man-made disasters in 2015: Asia suffers substantial losses*. Retrieved from http://media.swissre.com/documents/sigma1_2016_en.pdf

The Sendai Framework

In 2015, 185 countries adopted the Sendai Framework for Disaster Risk Reduction 2015 -2030[3] at the United Nations World Conference in Sendai, Japan. The Sendai Framework is a successor to the Hyogo Framework for Action (HFA) 2005-2015: Building the Resilience of Nations and Communities to Disasters. These frameworks assisted in shifting the emphasis from one of responding to disasters to taking an approach that focus on reducing future and existing disaster risk, and strengthening disaster resilience.

The Sendai Framework provides a welcome focus on CI with an emphasis to "promote the resilience of new and existing *critical infrastructure*, including water, transportation and telecommunications infrastructure, educational facilities, hospitals and other health facilities, to ensure that they remain safe, effective and operational during and after disasters in order to provide live-saving and essential services (p.21).

The United National International Strategy for Disaster Risk Reduction (UNISDR) further stresses the importance of CI through its "Making Cities Resilient: My City is Getting Ready" campaign."[4] Around the world over 3,000 communities have pledged to adopt strategies to increase their disaster resiliency, including adopting:

Essential Four: Pursue, Resilient, Urban Development, and Design – Invest in a maintain critical infrastructure that reduces risk, such as flood drainage, adjusted where needed to cope with climate change; and

Essential Eight: Increase Infrastructure Resilience – Protect ecosystems and natural buffers to mitigate floods, storm surges and other hazards to which your city may be vulnerable. Adapt to climate change by building on good risk reduction practices.

Critical Infrastructure in Canada

Public Safety Canada designates key partners and stakeholders in CI as fitting into ten sectors:

1. Health
2. Food
3. Finance
4. Water
5. Information & Communication Technology
6. Safety
7. Energy & Utilities
8. Manufacturing
9. Government
10. Transportation[5]

The importance of these stakeholders can be recognised in recent disasters in Canada.

The 2016 Fort McMurray Fire ultimately destroyed 2,400 out of a total of approximately 19,000 homes. Once all of the residents were safely evacuated, the efforts on the second day were focused on fighting the fire but also a prime consideration was to protect CI[6]. There was recognition that without CI in place, no-one would be able to return to the city of approximately 61,000 residents.

The 2014 Lac Mégantic train derailment resulted in 47 deaths, and about 2,000 people were evacuated. Specialised hydrocarbon recovery operations were required to deal with the 6.7 million litres of petroleum crude oil which spilled into the community's storm and sewer system affecting the ability of evacuees to returning to their homes.[7]

The 2013 Calgary flood resulted in major damage to the city's CI.[8] The Bonnybrook rail bridge was undermined and resulted in a train derailment and all other 20 bridges were closed. Calgary's downtown, the business heart of the city, was essentially closed; all routes into the core were flooded and transit service was suspended. Power was shut off to all evacuated areas, including the downtown. Power was not completely restored to the core until for eight days. The transit system took a hit as the waters damaged C-Train tracks in the Erlton area, flooded tunnels and undermined roads. The flooding resulted in costs estimated at $1.7 CA billion.

As can clearly be demonstrated, there is a great need to consider how CI can be designed to be disaster resilient and to minimise post-disaster recovery and rebuilding costs.

How can CI Experts be Helpful to Local Communities?

Let me start off by stating what is *not* helpful. Keep in mind that most disaster and emergency management (DEM) personnel do not have any university education or research skills in CI. Presenting information to local DEM personnel as if you were speaking before a graduate class, or as if writing for a peer-review journal, is not helpful. Complicated formulae are certainly important to your peers to identify the validity and robustness of your data and findings; but they are not understood, and thus not helpful to local DEM managers.

What is helpful? First of all, consider your work in a local or regional disaster context. Is what you are working on relevant to the planning for, responding to, or recovery from a disaster? If so, then you have to step out of your research lab, university or college office and reach out to those involved in DEM. You may need to start by increasing your own under-standing of the DEM planning process.

---

[3] UNISDR. (2015). *Sendai Framework for Disaster Risk Reduction 2015 -2030*. Geneva, Switzerland: UNISDR.

[4] UNISDR. (2016). *Making cities resilient: My city is getting ready*. Retrieved from http://www.unisdr.org/campaign/resilientcities/

[5] Public Safety Canada. (2015). *Critical infrastructure*. Retrieved from http://www.publicsafety.gc.ca/cnt/ntnl-scrt/crtcl-nfrstrctr/index-en.aspx

[6] CBC News. (2016, *May wildfire rages in Fort McMurray as evacuees settle in Edmonton.* Retrieved from http://www.cbc.ca/news/canada/edmonton/wildfire-rages-in-fort-mcmurray-as-evacuees-settle-in-edmonton-1.3565573

[7] Transportation Safety Board. (2015). *Railway Investigation Report R13D0054*. Retrieved from http://www.tsb.gc.ca/eng/rapports-reports/rail/2013/r13d0054/r13d0054.asp

[8] City of Calgary. (2014). *Calgary's most damaging flood*. Retrieved from http://floodstory.com/floods/2013-flood

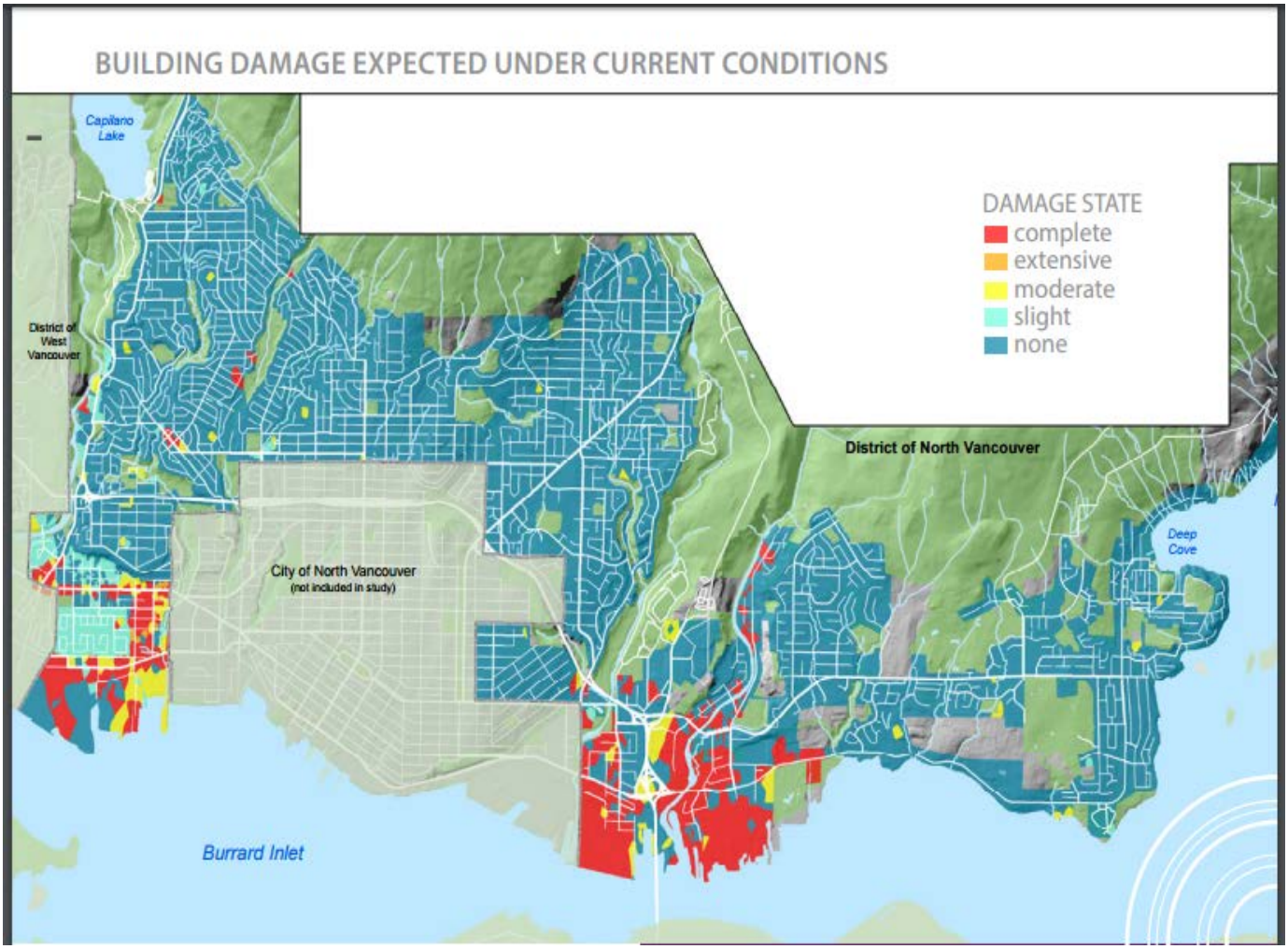


Figure 2: Building Damage Expected Under Current Conditions

1. What are the potential hazards that could affect the community? Don't just focus on the typical hazards such as floods, wildfires or earthquakes. Think about the full range of potential hazards.

2. How would these hazards affect the CI that you are interested in? What is the exposure of the CI? Is the CI located in soil that would liquefy following a major earthquake? Would the CI withstand a snow-melt flood? What would be the demands on CI if the community was affected by a heat wave or period of severe cold weather? What would happen if 50% of the maintenance staff were not able to come to work as a result of a pandemic?

3. Once you have a good understanding of how the CI would be impacted by the hazard, you then need to consider how businesses, residents and industry would be impacted. What are the short- and long-term consequences?

4. Given the various hazards, are the risks acceptable, tolerable or unacceptable? If they are unacceptable, then what mitigative strategies would increase the CI disaster resilience? If they are only just tolerable, how can the CI be strengthened?

5. If there are no known mitigation strategies and the risk is unacceptable, this should be identified as a research priority.

6. When mitigative strategies are identified, who is responsible for implementing the strategy? What is involved in implementing the strategy in terms of costs and length of time?

7. Now take the results of your analysis and write them out in non-technical language so they can be understood by DEM professionals. Use simple graphics to illustrate the problems. Describe the impacts as stories.

   For example, consider the recent effort by the District of North Vancouver [9] to illustrate the potential impacts of a major earthquake on CI (see Figure 1) and how it would affect various community residents:

[9] District of North Vancouver. (2016). *When the ground shakes. Earthquake risk in the District of North Vancouver and what we can do about it.* Retrieved from https://www.dnv.org/sites/default/files/edocs/when-the-ground-shakes.pdf

Henry is driving to his first customer of the day when his van starts to bounce. He looks in the rear-view mirror for potholes in the road, but his attention quickly returns to the road ahead as the cars in front of him screech to a halt. They don't all stop in time and some are rear-ended, while a few others jump the sidewalk and another crosses the centre line into oncoming traffic. Henry watches as a powerline leans slowly into the street and the power cable suddenly snaps, spraying sparks....

Henry's van is hemmed in on all sides with other vehicles. ... He can see almost every driver and passenger with a cell phone in their hand, but few have made a connection. He's not sure if he should try to help or walk back to Emma's daycare....

The stories are supported by complex analyses and GIS maps, but the report is written so that the impacts are clear to the average citizen.

8. Now you are ready to reach out to local DEM personnel and key stakeholders. Help them to understand what the issues are, and what you are concerned about. Advise them on ways to move forward; don't just leave them with the problem without some potential solutions.

   Consider how meeting the community's CI needs could be built into class project or would make an excellent graduate thesis. The next time you consider applying for a research grant, consider how the findings could be directly applied to help the community.

Perhaps this short article will stimulate your thinking and lead you to consider how you can:

1. Promote CI disaster resiliency.
2. Inquire as to what are the potential hazards.
3. Analyse your findings with a broad perspective – what does this mean to the citizens who live in the community?
4. Consult with peers to gain an appreciation of potential issues and solutions.
5. Encourage applied research to increase community disaster resiliency.
6. Reach out and share your findings and concerns with the local community.

No one knows when the next disaster will strike and who will be impacted it could be you and your family. The work that you do can contribute to your community's

1. sense of safety and calming,
2. self- and community efficacy,
3. social connectedness, and
4. hope.

SEZBC: Towards Situational Awareness in National Cyberspace

The goal of the project is to create a Cyberspace Security Threats Evaluation System (SEZBC) for national security management in Poland.

Cyber incidents pose a serious threat to governments, economies, businesses and individuals. Each country faces the problem of a growing number of serious attacks on essential computer networks. The first step to protect the national cyberspace is to improve situational awareness by continuous monitoring of critical infrastructure systems.

SEZBC project has been sponsored by National Centre for Research and Development and is carried out by the consortium of 3 entities: Military Communication Institute (leader), Enamor International Ltd. and PBP Enamor Ltd. Potential beneficiaries are Ministry of Digital Affairs, Internal Security Agency, Government Centre for Security and National Security Bureau.

EU has responded to this threat with policy and legislation proposals in the form of directives, plans and strategies [1][2][3]. Based on UE recommendations, national directives, acts, and programs have been incorporated (in Poland [4][5]). They emphasize that:

- Governments have a significant role in assuring a safe cyberspace, but since major parts of cyberspace are owned and operated by the private sector, cooperation between both sides is necessary.
- Each country should improve readiness and engagement of the private sector in cyberspace risk management in cooperation with the national authority for network and information security (NIS) (e.g. CERTs).
- There is a need for continuous monitoring of the national cyberspace that may be subject of cyber-attacks. The key cyberspace players like banking, energy supply, transport, Internet services as well as public administration should report incidents (identify, assess and manage the risks) to the national NIS competent authorities to enable common cyber situational awareness for decision makers.

National CIIP

Polish National Critical Information Infrastructure Protection assumes shared responsibility for the risk management across all levels of government and critical infrastructure owners and operators. In Poland a set of 11 systems, which have fundamental importance for the national security and comprehensive operation of the country has been identified. The full list includes:

- Energy, fuel and energy supply system,
- Communication system,
- Tele-information network system,
- Financial system,
- Food supply system,
- Water supply system,
- Health protection system,
- Transportation system,
- Rescue system,
- System ensuring the continuity of public administration activities,
- System of production, storing and use of chemical and radioactive substances, including pipelines.

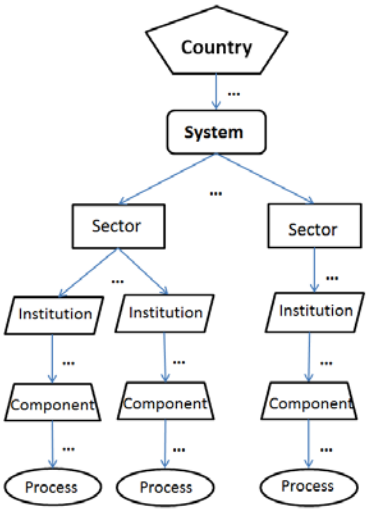


Figure 1

Each system may be composed of Sectors, Institutions, Components and Processes (Figure 1). The list of critical infrastructure elements is not available to the public.

J.Śliwa

Dr. J.Śliwa is a head of C4I Systems department in MCI. She has been responsible for SEZBC concept and architecture design .
e-mail: **j.sliwa @wil.waw.pl**

R.Piotrowski

Dr. R.Piotrowski is a researcher in MCI and as a Project Manager of SEZBC he has been involved in all phases of the project.
e-mail: **r.piotrowski @wil.waw.pl**

P.Berezinski

Dr. P.Berezinski is a researcher in MCI. He has been involved in implementation phase of SEZBC.
e-mail: **p.berezinski@wil.waw.pl**

SEZBC

SEZBC is a country-level cyber security evaluation system with decision support. It incorporates risk assessment and risk management functions together with situational assessment. In particular, SEZBC supports decision making process in evaluation of the state of emergency in case of large-scale cyber-attack/incident or high risk of cyber threats' materialization. This system supports what-if analysis for simulating potential threat escalation as well as testing the results of different mitigation options. Incidents' acquisition in SEZBC is supported by cyber-threat catalogue based on CAPEC [7].

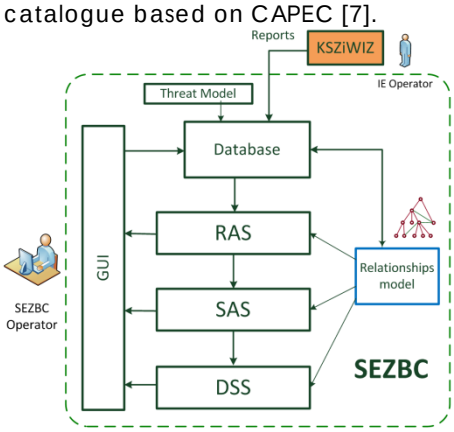


Figure 2

Analysis performed by SEZBC is done bottom-up based on relationships Model, a weighted graph where relations between nodes (Systems, Sectors, Institutions, Components, Processes) are modeled (according to National CIIP) and which maps the importance of particular entity to the operation of the whole country.

The heart of SEZBC is Risk Assessment Subsystem (RAS), see Figure 2. It employs an algorithm which takes into account system vulnerabilities (potential threats, possible effects resulting from threat materialization and security mechanisms used for attack counteraction) measured periodically by critical infrastructure elements' administrators, and incidents identified by security controls. Constituent parts of aggregated risk metric are propagated according to the predefined Relationships Model (Figure 3).

The results of Risk Assessment augmented with additional information on the effects of potential and actual attacks on the life of people and operation of the country are the input to Situation Assessment Subsystem (SAS). It evaluates the situation in terms of the impact of events on the life of the citizens and is able to recommend special organizational measures if necessary (e.g. crisis

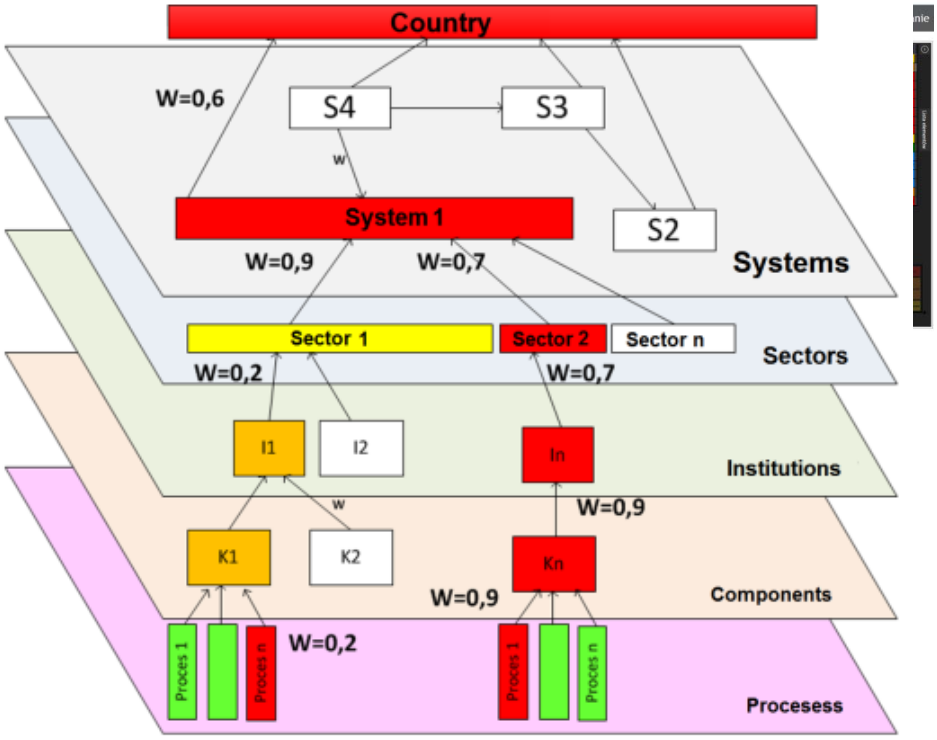


Figure 3

management, declaration of state of emergency or martial law). The effects of cyber-attack in real life are evaluated by a person responsible for attack/ incident reporting. The value of SAS recommendation is strongly dependent on the quality of input information (reliability of the Relationships Model and its parameters, precision of the systems' vulnerability level assessment and potential threats identification, assessment of the effects on a real life). Based on the national law, alarm states are grouped into 3 categories: emergency, natural disaster and martial law.

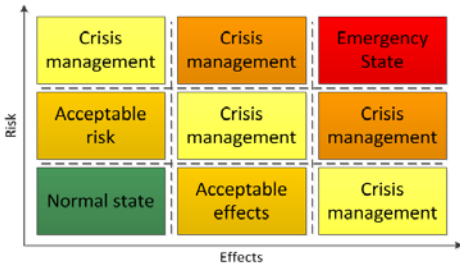


Figure 4

Decision Support Subsystem (DSS) provides visualization and reporting of RAS and SAS results and enables to recommend possible reactions on the actual situation (on the country level) as well as simulate different decision scenarios. It is designed to support top-level decision makers yet allows to drill down into technical details in order to deeply investigate each threat (Figure 5).

SEZBC operates mainly on external data entered by the operators of the infrastructure. A proxy between SEZBC and other data source elements was called KSZiWIZ (Figure 2). In the current implementation it offers an application to be used by public administration (all levels), critical infrastructure operators, and business sector. However in the future it has been proposed to develop a specially tailored system for exchange of information between key cyberspace players, giving them the possibility to access cyberspace situational awareness on their level of responsibility and provide value-added early warning.

Conclusions

Figure 5

SEZBC integrates information from cyberspace monitoring on the country level and, in this terms our approach, is quite new and unique. The goal of the project was to prepare the pilot deployment enabling evaluation of cybersecurity threats of the Republic of Poland cyberspace. Successful deployment will enable improvement of cyber situational awareness and decision support

for administrative units responsible for the national security.

Deployment of such a system demands a lot of effort and up to now it still leaves open issues, problems and challenges. Firstly, how to acquire all information to build and maintain (keep it up-to-date) comprehensive Relationships Model. Secondly, how to attract private sector to share data about risks and incidents which they observe in their systems and networks they are responsible for. This information is usually very sensitive and may be used against the company, resulting in the loss of reputation. In this aspect the institutions collecting such sensitive data must be in a position of an unlimited trust.

Thirdly, how to ensure that only reliable and up-to-date information from data source elements feed the system. This is the key requirement for the proper SEZBC operation and its ability to present actual situation.

References

[1] Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT, THE COUNCIL Brussels, 7.2.2013 JOIN(2013) 1 final

[2] EU Cybersecurity plan to protect open internet and online freedom and opportunity - Cyber Security strategy and Proposal for a Directive

[3] Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL concerning measures to ensure a high common level of network and information security across the Union, {http://ec.europa.eu/maritimeaffairs/policy/maritime_spatial_planning/documents/swd_2013_65_en.pdf}

[4] Cyberspace Protection Policy of the Republic of Poland, Warsaw, 25 June 2013,

[5] National Critical Infrastructure Protection Programme, http://rcb.gov.pl/eng/?p=79

[6] Description of Project "Cyberspace Security Threats Evaluation System of the Republic of Poland for national security management", project No DOBR-BIO4/011/13221/2013,

[7] Common Attack Pattern Enumeration and Classification (CAPEC), Mitre Corporation, https://capec.mitre.org/ .

The 52nd ESReDA Seminar On Critical Infrastructures: Enhancing Preparedness & Resilience for the security of citizens and services supply continuity

52nd ESReDA seminar will be held on May 29-31, 2017 in Lithuania

Announcement and Call for papers

Critical Infrastructures Preparedness and Resilience (CIP&R) is a major societal security issue in modern society. Critical Infrastructures (CIs) provide vital services to modern societies. Some CIs' disruptions may endanger the security of the citizen, the safety of the strategic assets and even the governance continuity.

The critical role that CIs play in the security of modern societies is a direct effect of the ever-increasing spread out of the information technology (IT) in every smallest task in man's daily-life. The continuous progress in the IT fields pushes modern systems and infrastructures to be more and more: intelligent, distributed and proactive. That increases the productivity, the prosperity and the living standards of the modern societies. But, it increases the complexity of the systems and the infrastructures, as well. The more complex a system is, the more vulnerable it will be and the more numerous the threats that can impact on its operability. The loss of operability of critical infrastructures may result in major crises in modern societies.

To counterbalance the increasing vulnerability of the systems, engineers, designers and operators should enhance the system preparedness and resilience facing different threats. Much interest is currently paid to the Modelling, Simulation & Analysis (SM&A) of the CI in order to enhance the CIs' preparedness & resilience.

The European Safety, Reliability and Data Association (ESReDA) as one of the most active EU networks in the field has initiated a project group (CI-PR/MS&A-Data) on the "Critical Infrastructure/Modelling, Simulation and Analysis – Data". The main focus of the project group is to report on the state of progress in MS&A of the CIs preparedness & resilience with a specific focus on the corresponding data availability and relevance.

In order to report on the most recent developments in the field of the CIs preparedness & resilience MS&A and the availability of the relevant data, ESReDA will hold its 52nd Seminar on the following thematic: "***Critical Infrastructures: Enhancing Preparedness & Resilience for the security of citizens and services supply continuity***".

Topics

Threats identifications & specifications
CIs disruptions MS&A
CI's vulnerability MS&A
CIs' dependencies and interdependency MS&A
Data and Databases
Emergency and crises management models & tools
IT inferences on CIs preparedness & resilience
Standards & Ontology in the domain of CI protection (CIP)

Critical Infrastructures Sectors

Air-transport & airports
Electrical power generation & supply
Gas & Oil production, storage & transport
ICT networks
Massive data storage & servers
Maritime transport & ports
Medical & health care
Process industry
Railway transportation
Supply chain process
Water supply and water works

Threats

Extreme weather conditions
Natural threats
Earthquake
Flood
Forest fire
Landslide
Torrential rain
Tsunami
Volcanic eruptions
Industrial & technological accidents
Financial & stock market perturbation
Wastes disposal

www.esreda.org/event/52nd-esreda-seminar/?instance_id=39

BIPSE: Cyber security in Industrial Control Systems

BIPSE system offers a complex and effective protection of the Industrial Control Systems' (ICSs) information infrastructure from cyber threats

The Critical Infrastructure (CI) of a country is usually defined as the one providing essential services for the society, serving as a backbone on the nations' economy, security and health. According to National Critical Information Infrastructure Protection Program [1] in Poland it includes several systems, among which there are: power and fuel supply, communications, financial, food supply, water supply, health protection and transportation. CI plays a key role in the state operation and influences the lives of the citizens. Serious systems' disruptions or damages caused by natural forces or as a consequence of human activities can generate significant losses for the citizens and the economy.

SCADA

Power supply processes are realised hierarchically, from the level of the power plant, through the energy transfer grid, controlled by the Central Control System (CCS), to the distribution systems. They are controlled by the Supervisory Control And Data Acquisition (SCADA) systems. In the past, SCADA systems ran over dedicated analogue lines and networks with vendor specific protocols, hardware and software. The network for power generation control was isolated from the public network.

Today's SCADA systems take advantage of open transmission protocols, broadly used in communications networks together with computers running common operating systems that work as the base for Intelligent Electronic Devices (IEDs). This significantly improves automation efficiency and decreases costs spent on control systems, but certainly it also increases the risk of system vulnerabilities' exploitation and influences its security level.

Nowadays SCADA control commands and responses flow across IP-networks and over IP-stack. As a result, control systems such as SCADA, power transmission management system, centralised Load Frequency Control (LFC) System, intelligent field devices (e.g. Remote Terminal Unit located in the Control and Supervisory Substation (CSS)) or IEDs, create new concerns for the cyber security.

BIPSE System

In response to these threats, we have proposed and developed a CI Security System that is to ensure secure IP-communications within the power grid management network [2]. BIPSE cybersecurity system prototype provides:

- analysis of the network traffic, searching for threats and anomalies;
- detection of malicious actions using specially designed IED-emulating probes;
- correlation of events flowing from the sensors;
- automated detection and tracking of threats, giving appropriate response measures;
- management of the ICT infrastructure security (stations and technological communication);
- cyber situational awareness of the whole monitored CI (SIEM – like).

BIPSE system was developed by the consortium of four entities: Military University of Technology (leader), Research and Academic Computer Network, Military Communication Institute and Asseco Poland S.A. within the research project sponsored by the National Centre for Research and Development.

In particular, the security measures used in the BIPSE system are:

- authentication;
- advanced access control, e.g. with the use of ABAC model and security policies;
- anomaly detection and filtering of management and control IP traffic transferring IEC protocols;
- encryption of BIPSE management messages;
- monitoring of the status of the protected infrastructure and secure storage of information;
- honeypots and SCADA hardware emulation;

Marek Amanowicz [1]

Professor and Project Manager responsible for coordination of the entire work and cooperation with the customers.

marek.amanowicz@wat.edu.pl

Jacek Jarmakiewicz

Dr. Jarmakiewicz responsible for BIPSE system architecture design, framework tests, system verification and validation.

jacek.jarmakiewicz @wat.edu.pl

Adam Kozakiewicz [1]

Dr. Kozakiewicz, the Architect of the project, responsible for BIPSE reference architecture.
e-mail**: adam.kozakiewicz@nask.pl**

Joanna Śliwa

Dr. Śliwa, responsible for validation of the IEC 104 probe and engineering access control.
e-mail: **joanna.sliwa@wil.waw.pl**

- secure communications with the central SIEM and GUI;
- audit and traceability of management operations, and detection of potential unauthorised operations.
- HoneyPots, SCADA HoneyNets and DarkNets for monitoring and logging of all of the suspicious activities in ICS network;
- Mediation Device developed to normalise the messages obtained from the other security systems and elements;
- SIEM System gathering, analysing and aggregating information received from abovementioned elements;
- databases gathering the history of power control and management conditions;
- Cyber security Visualisation and Management System processing data produced in SIEM in real-time;
- engineering access control system for monitoring and control of all technical service activities – including video registration.

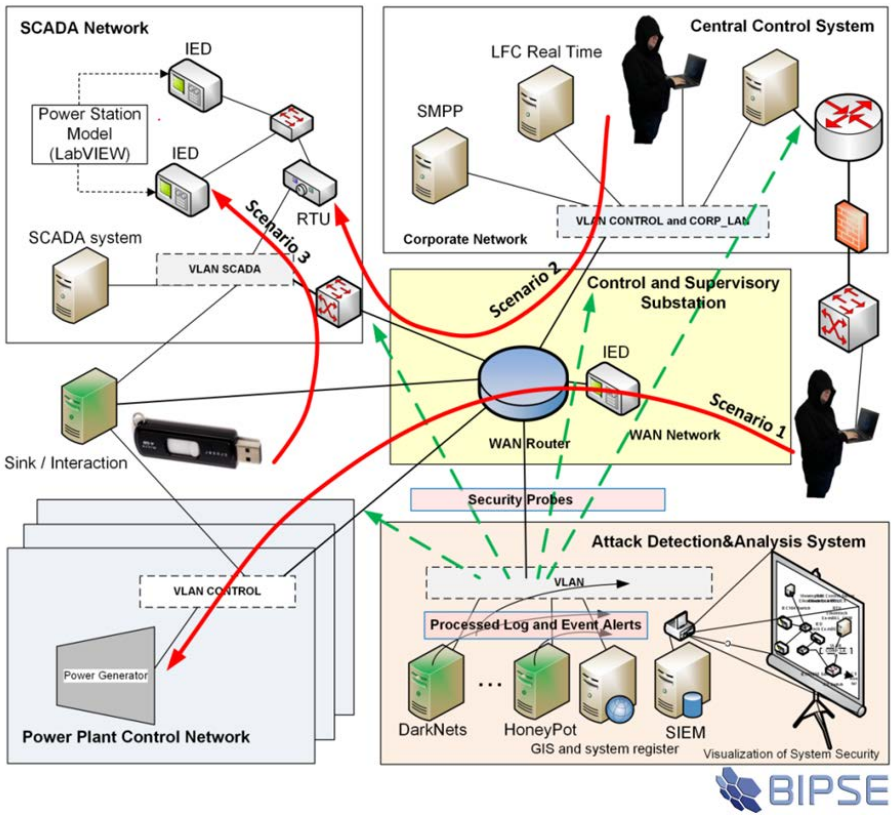


Figure 2. BIPSE test scenarios

BIPSE system evaluation

Functional tests of the system have been performed both in the consortium-owned laboratory environments [3] resembling the architecture of power stations as well as in the Laboratory of Distributed Generation at the Lodz University of Technology [4].

The experiments were designed to verify the ability of the system to detect cyber-attacks and to protect against them, as well as to adjust the sensitivity of probes and decoys developed in the project.

We intended to verify the efficiency of threat detection by tools developed by us, i.e.:

- probes based on Snort and Bro software that are adapted for analysis of the SCADA protocols (e.g. IEC 60870-5-104) in order to detect anomalies in the power control and management systems;
- commercial IDS/IPS probes that were previously purchased and are currently used in the power control and management network;

Test scenarios (see Figure 1) defined the following directions of attacks:

- from the Internet and over WAN with the use of unauthenticated and unauthorised measures by intruders;
- from the enterprise network, the attacks coming from authorised users of this network who, due to various reasons, attack the power control system;
- from the control network by persons who know the effects of the attacks and due to personal and/or external reasons conduct attacks on the infrastructure;
- from the control network by users who are not aware of the threats, authorised to resources (e.g. during a software update a malware is installed and transferred along with the useful software).

Conclusions

The positive results of the BIPSE validation allowed for its installation in the power station of the Polish Transmission System Operator PSE S.A. Exhaustive tests performed in real operating environment confirmed that BIPSE system meets all functional requirements. Its specific features like modular and scalable architecture, closed-loop reaction to detected threats, expanded engineering access control subsystem, and lack of negative impact on security and reliability of the protected object allows the system adaptation both to small and large-scale implementations. BIPSE system can be also adapted to other critical infrastructure environments, such as fuel or water supply systems.

The advanced concept of BIPSE system covers a trusted multi-domain cooperation when the domains share the identified threat information building a cybersecurity situational awareness picture of the power supply process.

References

[1] National Critical Infrastructure Protection Programme,

[2] Description of Project "Cyber security provision system for critical infrastructure", project No. DOBR/0074/R/ID1/2012/03

[3] J. Jarmakiewicz, Development of Cyber Security Testbed for Critical Infrastructure, 2015 ICMCIS, IEEE Explore DOI:10.1109/ICMCIS.2015.7158686

[4] Laboratory of Distributed Generation – Institute of Electrical Power Engineering, Lodz University of Technology http://www.i15.p.lodz.pl/pl/pliki_htm/LGR.htm

CUIng: Criminal Use of Information Hiding Initiative

The goal of the Criminal Use of Information Hiding Initiative is to combine expertise and experience from academia, industry, law enforcement agencies and institutions to tackle the increased utilisation of information hiding techniques and prevent its wider diffusion.

Current malware is increasingly using various types of information hiding techniques (like steganography) to avoid detection and hide communication and (confidential) data exfiltration. This new trend is confirmed by the latest examples of malicious software with information hiding capabilities, e.g., *Hammertoss*, *Stegoloader*, *Regin* or *Duqu*. Information hiding has been utilised by cybercriminals but also other actors such as spies (e.g., the Russian spy ring discovered in the US in 2010) and terrorists (e.g., members of al Qaeda arrested in Berlin in 2012 were in possession of video files containing hidden information). Information hiding techniques have also been used by insiders to exfiltrate sensitive data.

„The creation of new narrow-focused initiatives like Criminal Use of Information Hiding (CUIng) allows to investigate and share threat intelligence on various cybersecurity aspects and to develop more effective solutions"

Considering the sophistication of the techniques found in the wild, the authors believe that there is an urgent need to act at EU-level. To this end, the **Criminal Use of Information Hiding (CUIng)** initiative was launched in cooperation with Europol's *European Cybercrime Centre* (EC3). Working jointly and combining expertise and experience from academia, industry, law enforcement agencies and institutions, the initiative aims to tackle the threat posed by the criminal use of information hiding techniques while it is still characterised by a limited adoption.

Main Objectives

The five main objectives of the proposed initiative are:

Raise Awareness: inform about the threat that information hiding techniques can pose. Especially: increase the sensitivity to cybercriminals' potential for information hiding exploitation (e.g., in companies) and emphasize how forensic investigations could become significantly more challenging in the presence of such techniques.

Track Progress: monitor sophistication and complexity of information hiding techniques found in the wild used by cybercriminals, terrorists and other actor groups.

Share Threat Intelligence: bring together security professionals from government institutions, academia, law enforcement and industry to distribute information and share experience and expertise from different viewpoints

Work Jointly: cooperate and benefit from joint potentials to develop effective countermeasures and integrate them on a global scale (or at least EU level).

Educate & Train: ensure that law enforcement agencies, companies, institutions, individuals, etc., will be ready and fully prepared to react against potential cybercriminals' information hiding exploitation.

Benefits

Depending on the type of the partner involved in CUIng, various benefits can be identified:

For academia, the main benefits include more chances to support other partners in better understanding

Wojciech Mazurczyk [1]

is an Associate Professor at Warsaw University of Technology, Poland. He is a coordinator of CUIng.

wmazurczyk@tele.pw.edu.pl

Philipp Amann

is the Senior Strategic Analyst of the European Cybercrime Centre (EC3) and Head of the Strategy and Development team.

Philipp.Amann@europol.europa.eu

Luca Caviglione [1]

is a Researcher at the National Research Council of Italy.

luca.caviglione@ge.issia.cnr.it

Steffen Wendzel

is head of a research team at Fraunhofer FKIE, Bonn, Germany, and author of five books.

steffen.wendzel@fkie.fraunhofer.de

information hiding-based threats as well as taking part in the development of more effective countermeasures.

It also improves awareness of professionals and researchers. In addition, CUIng fosters the competetiveness of European researchers in this domain, for instance through media coverage, participation in significant events and relevant publications (books, special issues for journals, papers, etc.)

For industry, the main benefits are a better evaluation of related threats and risks, and the facilitation of new markets focusing on data leakage protection and anti-malware information-hiding-aware solutions. Eventually, this will lead to an improved protection of the sensitive business data.

Law enforcement agencies can take advantage by consulting and informing the public and other partners about the potential risks related to information hiding threats. They can become more aware on the evolution of such techniques and adjust their subject-matter specific knowledge for investigations and the work of digital forensic analysts.

For institutional partners, the key gain will be a better understanding of the threats and risks involved. This improved awareness should impact on product and tool selection, IT configuration and training activities. In addition, the improved know-how on protection against hidden data leakage will help to secure critical assets, including intellectual property.

CUIng Structure

The initiative welcomes all interested members from different backgrounds to participate in CUIng.

The structure of the initiative consists of the Steering Committee and regular members. The Steering Committee is responsible for setting the strategic direction of the initiative and proposing, approving and coordinating all its activities. The Steering Committee is a mix of members from academia, industry, LEAs and institutions. Currently, it is composed of seven members from Canada, Germany, Italy, Poland, The Netherlands, and the United Kingdom.

Current Activities

The initiative uses the Europol Platform for Experts' EC3 - SPACE as a place for collaboration, networking, planning future activities and sharing information. It will provide a common environment to express views and to discuss pertinent trends. It also provides an up-to-date repository of relevant reports, publications and documents on criminal use of information hiding techniques.

The initiative gathers and shares the following information:

- **General background on information hiding**: provide a general overview on the topic,
- **Scientific publications**: relevant papers (mostly surveys), which present the state-of-the-art in academic research in information hiding,
- **Information hiding-capable malware**: analyses of real-life malware that utilises information hiding techniques. Reports are mostly delivered by security professionals from anti-malware companies and share specific details on the modus operandi.

Members have been co-organising and taking part in various events (conferences and workshops) to promote the initiative and to attract potential new members. Recently, CUIng has been a program partner and will be presented at the 2016 eCRIME conference in Toronto, Canada, and at the 2016 DeepIntel conference in Schladming, Austria. Some past events that provided an opportunity to promote the initiative was mentioned include: "Emerging and Current Challenges in Cybercrime and Cyberterrorism" (March 2016, The Hague, Netherlands) and "Secure Europe without borders" (February 2016, Lodz, Poland).

CUIng also helped Europol's EC3 to create a CyberBit, a brief backgrounder for the Trends Series entitled "Steganography for increased malware stealth". CyberBits are intelligence notifications on cyber-related topics that aim to bring important facts and findings to the attention of the cyber community in a timely manner to raise awareness and to trigger discussions or further actions.

The CUIng Community

The members of the initiative firmly believe that working together allows building a robust community taking advantage of expert knowledge and expertise from academia, industry, law enforcement and institutions. This network approach, leveraging different communities, should alleviate the problem of the criminal use of information hiding techniques before it becomes a widespread phenomenon.

If you would like to find out more about CUIng or become a member of the initiative, please visit our website at: **cuing.org** or email us at: **info@cuing.org**.

NASK's experiences with actionable information and threat intelligence

CERT Polska is a division of NASK that secures the .pl domain and Polish networks. Dealing with actionable information is our bread and butter, as we handle incidents reported by users of Polish Internet and threat intelligence from our contacts from all over the world. Utilising threat data feeds in our daily operations and projects gives us unique insight on usability of threat intelligence information available in the security community.

What is actionable information?

For an incident response team (CERT / CSIRT) actionable information is information on all aspects of network security incident that are relevant to the incident and its possible handling. It can be a list of IP-addresses, a dump of traffic captured between malware installed on an infected computer and its C&C server, a hash of a malware sample or the sample itself. In the modern world of network threats, the possibilities are endless. For the information to be actionable, though, it has to meet the following criteria: **relevance**, **timeliness**, **accuracy**, **completeness** and **digestibility**. Let us take a closer look at these attributes:

Relevance means that the information must be related to the attack and relevant for the receiving party (for example, response team's constituency). Information that is not a description of an incident is not considered as actionable. Description of an attack affecting someone on the other side of the globe is not actionable for a team tasked to protect a single organization (or any other well-defined constituency).

Timeliness affects relevance of the information. With the attacks being carried out in real time, most of their characteristics can change rapidly, making the old information irrelevant. For example, it is quite common for malware to switch C&C domains in quick succession.

Accuracy of the information is crucial (as we will show in the "Lessons learned" section). Errors in the data can lead to false positive detections when the data is used to detect threats, or can hinder the investigation of an incident.

Completeness of the information must be considered in the wider context of the data exchange. Leaving out something can make the information unusable, but it may be due to confidentiality rules, laws or agreements which can limit scope of the information to be shared. There is no rule of thumb of information completeness.

Digestibility means that the information needs to be in a form allowing it to be easily imported into organisation's information management systems, and then transformed, shared and/or used.

Our projects

Our experience comes from dealing with actionable information and threat intelligence in the course of following projects:

n6 platform

The n6 platform is the core of our operations. Its name is a wordplay on the Network Security Incidents Exchange acronym. The system is a threat intelligence and actionable information sharing platform developed by NASK. In 2015 it handled a record number of more than 200 million notifications of threats in Polish address space. The platform shares the data through an application programming interface (API) based on HTTPS and RESTful architecture. There is also a supplementary interface using STOMP protocol for streaming the data, minimising the delays that often occur when other methods of data exchange are employed.

Janusz A. Urbanowicz

Janusz A. Urbanowicz is a senior security projects specialist at NASK. Before that he built a commercial CERT, designed security featured in cloud products and managed incident handling for a major Polish university.

He lately co authored a paper on cyber-attacks attribution: "The Never-Ending Game of Cyberattack Attribution" with Piotr Kijewski, Przemek Jaroszewski and Jart Armin, and he is working on malware defense systems for the financial industry.

email: **Janusz.Urbanowicz@cert.pl**

Additionally, we have provided the users an ability of receiving periodic notifications when new information about their networks is available. The threat intelligence data stored in n6 platform comes from our research, from open data sources available on the Internet and from other organisations working with threat intelligence and actionable information.

ILLBuster

ILLBuster[10] is an another project based on utilising actionable information. The purpose of the project was to develop an automated system for detection and analysis of harmful websites. The project was developed by consortium led by Università degli studi di Cagliari and Università degli studi di Milano-Bicocca and thus the system operations are focused on the Italian Internet. The developed system detects suspicious domains using fast-flux detection technology and an automated crawler analyses the websites. The crawler detects advertisements of: sales of illegal goods, child pornography, phishing and malware. The ILLBuster system is both a producer and consumer of actionable information. It consumes n6 data about Italian networks and produces information as report of the analyses and detected suspicious domains which are reported back to the n6 platform.

FlowSense

FlowSense is a network threats detection software, operating on metadata only. FlowSense uses open source Argus [11] engine to analyse network traffic to extract flow information, then correlates it with threat intelligence from the n6 platform. The FlowSense solution gave us most experience with using threat intelligence in the real world.

Lessons learned

In our work with threat intelligence feeds we utilise them from various sources of information from all over the world. These sources are usually feeds of data coming from automatic analysis of malware or spam, by registered connections to sinkhole systems and found by other means that are sometimes not publicly disclosed. While the data from sinkhole systems are reliable, other means of creating feeds often could be not reliable enough.

As an example, we have received reports of phishing pages, that indicated real bank websites. We do not know how it was determined that the page hosts a phishing website. We may hypothesise that this is a false positive from an automated system that determined falsely that the actual bank page is a phishing page targeted at the bank.

Such cases stress out that there is a strong need to verify that the incident report is accurate. The verification method should be automatic, since it allows for processing the massive amounts of automatic threat reports. It is, however, the fallibility of automatic reporting and verification that is the reason for the need for verification, creating a chicken and egg problem.

Another danger comes from interaction of data enrichment process with social network design patterns. Social networking platforms commonly use URL shorteners to keep track of users clicking URL addresses shared as social content. As malicious URL-s are also shared through social media, and as a result of this processing often reported in shortened form, it associates the domain name of URL shortening service with malicious content. This leads us to assumption, that data enrichment procedures often do not follow the reported links to establish the real malicious URL.

Another pitfall lies in the data enrichment process. Our n6 platform routinely adds metadata to reported URL-s and IP addresses. For example, if the URL redirector or shortener is operated by a social network, its domain name resolves to its operator IP address range, usually serving the whole infrastructure, and not only the shortener. If this IP-address is then stored along the URL and used in malicious IP-addresses blacklist, chance is, any connection to a social network infrastructure will be marked as suspicious or blocked. Real life example is that supplanting a goo.gl shortened URL with the domain name IP-address will lead to marking at least some connections to Google services as connections to a malicious IP-address. This kind of false positive is created by automatic data enrichment without taking account of nature of the data item.

Another trouble lies in threat intelligence concerning malicious pages. Our research especially during the ILLBuster and earlier HSN/HSN2 projects shows that it is practically impossible to automatically and reliably determine if a URL is used to infect visitors with malware. While HSN/HSN2 is able to detect some common web exploits, most available automatic detection tools require a knowledgeable human operator to guide the analysis and interpret the results, especially as modern exploit kits employ various strategies in order to defeat automatic analysis. One such technique employed by exploit kit operators is to set DNS records for a domain which was used for nefarious purposes so it resolves to an invalid IP-address when no longer needed, for example to 0.0.0.0, or to an address within a private address space, making analysis of the malicious content previously hosted on that domain impossible and sabotaging the workings of automatic analysis tools.

Other exploit kit tricks include leading the victim's browser through a maze of ever-changing redirections, setting cookies and blacklisting importunate IP-addresses that are used by the analysts to crack the workings of an exploit kit. In practice, it takes a sizable amount of an analyst's work (measured in days) to trigger the exploit kit to take a malware shot at the analyst's browser.

Those experiences led to implementation of "confidence" metrics in our n6 platform. Users of the platform can select confidence level of the source when querying the platform for data, to avoid false positives and low-quality automatic feeds data. The confidence score is (high, low or medium) is assigned due to observed quality of data coming from a given source.

Standards are great, there are so many of them to choose from

An apex of our work with actionable information was development, on commission from European Network Security Agency, a set of guides for utilizing actionable information in

[10] For more information about ILLBuster project visit http://illbuster-project.eu/

[11] http://qosient.com/argus/

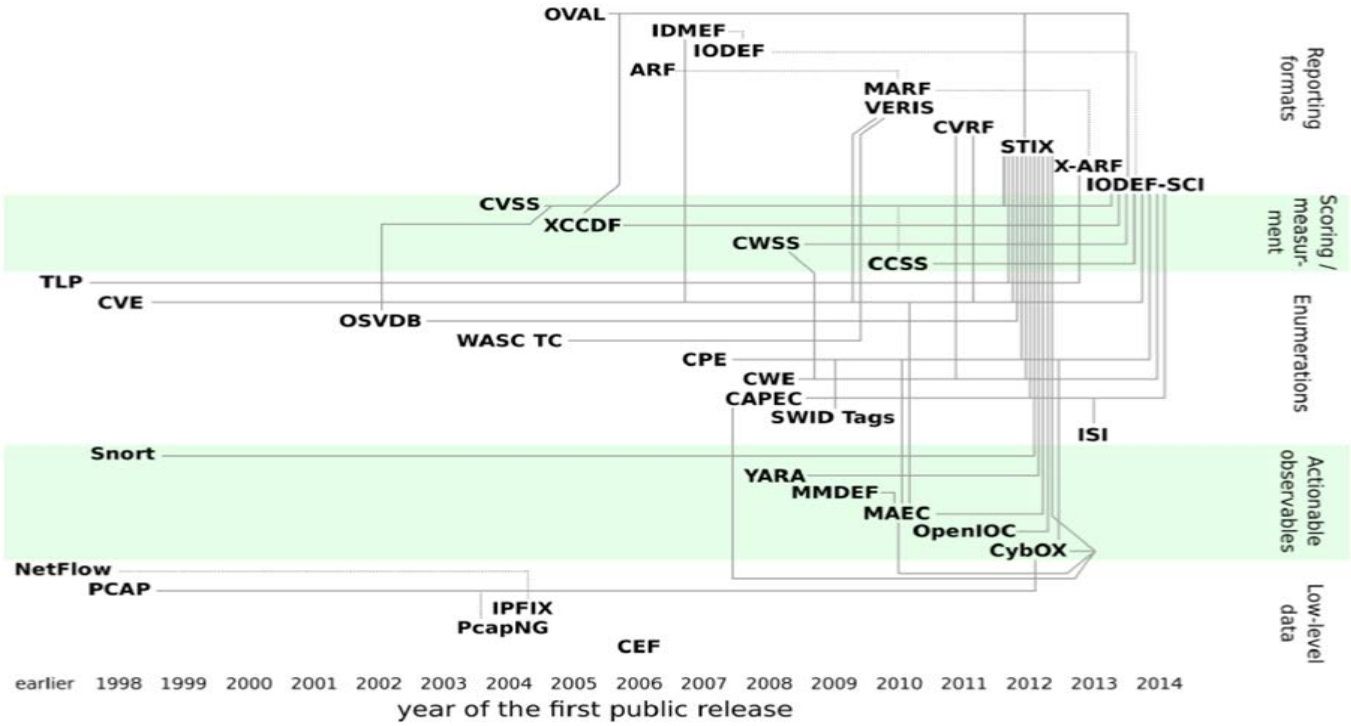


Figure 1 - Relationship and development tree of actionable information standards. Source: "Standards and tools for exchange and processing of actionable information", ENISA, 2014

CSIRT operations. We have catalogued 36 formats and standards for dealing with various aspects of actionable information. This abundance makes it quite complex to determine which formats and standards should be used [12] . The complexity we discovered while researching the formats and standards is presented as Figure 1, and new formats were introduced only after we finished the research.

Conclusion

Threat intelligence and actionable information sharing are one of the most important aspects of fighting Internet threats, as no single actor can secure the whole Internet. At NASK we developed significant capability in dealing with actionable information – our n6 platform distributes relevant actionable information to Polish network operators, and is free to access if you are one. Yet is not trivial both to create and consume actionable information and from our experiences it is a dangerous thing to rely on received actionable information only to detect and block internet threats. Further research on ensuring its quality and validity is needed.

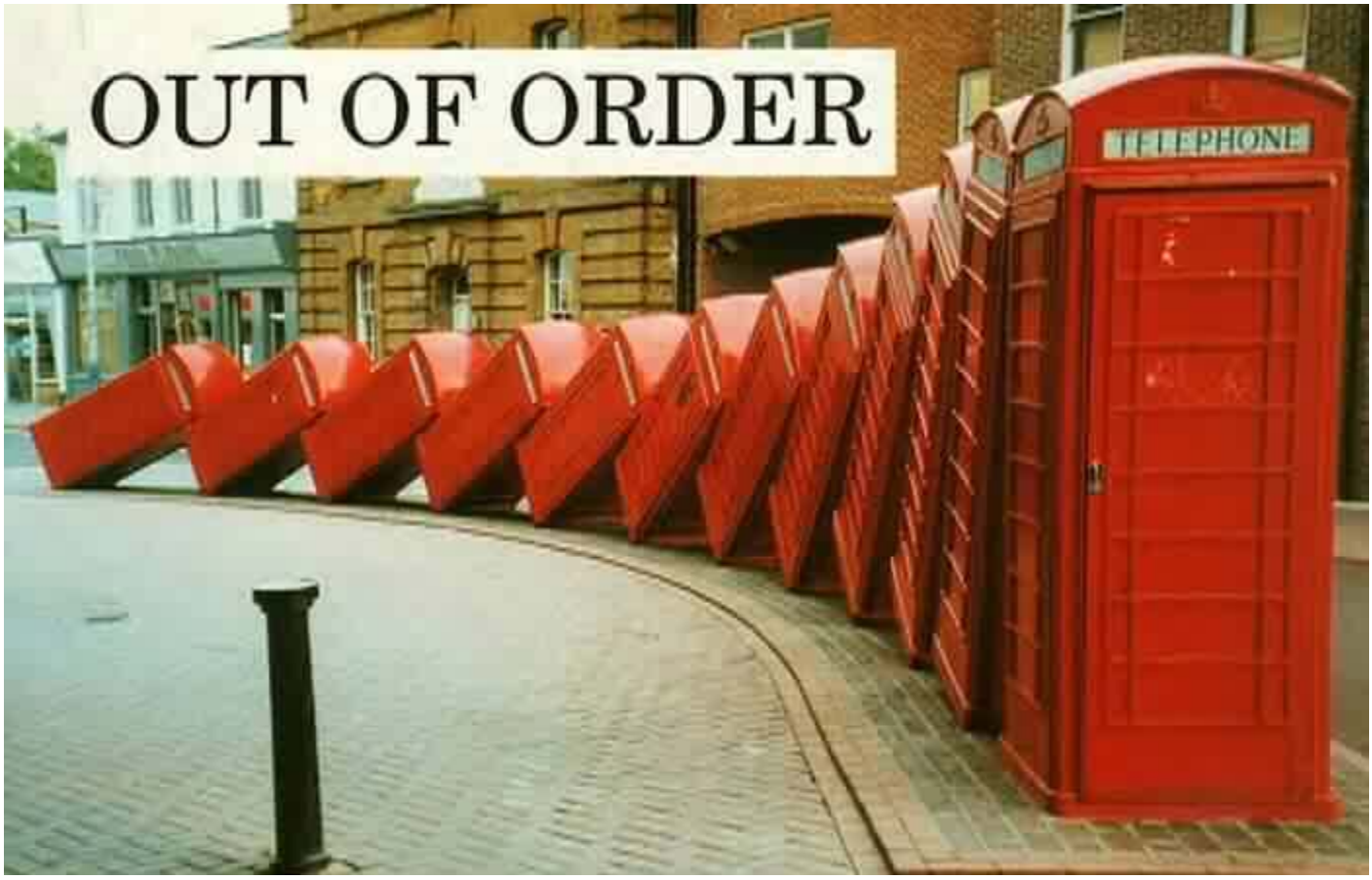
[12] For the full set of ENISA actionable information guides, see https://www.enisa.europa.eu/news/enisa-news/new-guide-by-enisa-actionable-information-for-security-incident-response

Joint final conference of projects on cascading CI Effects

CASCEFF, CIPRNet, FORTRESS, PREDICT, SNOWBALL

March 16 and 17, 2017

save the date



The **joint final conference** place t.b.d on the **16th of March** 2017 (full day) and in the morning of **17th of March** 2017 (1,5 days)

In the **afternoon of the 17th of March** a kind of **joint wrap-up session** is held together with **Joint Research Centre's (JRC) Disaster Risk Management Knowledge Centre (DRMKC)** event. This will be a summary session where main conclusions of both events will be presented to Policy DG representatives and inviting them to react from a policy viewpoint.

Follow on

www.ciprnet.eu

All-Hazard Training

How to exploit sophisticated simulation environment to improve the training to manage complex crisis situation: the experience of the students of the Master in Homeland Security (Italy) using the 'what-if' analysis tool of EU project CIPRNet

There is no doubt that the security of a country is measured also by its capacity to prevent, counter and recover from a catastrophic event. Natural disasters, social tensions and the upsurge of criminality and terrorism constitute threats that can seriously undermine the social, political and economic development of a country. Such threats must be analysed recognising that their targets, CI especially, are part of a system that is itself intertwined with other systems. This is why it is crucial for security experts from both private and public sectors to approach security in a holistic manner, as this will in fact preserve the country's overall development and prosperity.

Today, citizens demand and are rightfully entitled to higher security standards. It is therefore in the interest of every nation to ensure that governmental institutions and private companies, whose services are deemed essential to citizens, acquire all the necessary tools to win these new fights.

Throughout the world, in recent years, we have witnessed criminal or terrorist attacks that have had a high impact on the media and the population. People's perception of safety and security have been badly shaken. However, even though such events have had the capacity to frighten the population and feed a strong sense of mistrust towards the institutions that are responsible for its protection, a whole new type of threats, much more insidious and damaging, has recently emerged. In fact, we are facing new phenomena such as cyber-attacks to state institutions and infrastructures (e.g. the cyber-attacks to Estonia in 2007), disclosure of strategic military or diplomatic information (e.g. The Snowden case in 2013), personal identity and personal data thefts, industrial espionage and technology theft.

International concern is growing. This led some international organisations to take concrete action. NATO, at the recent Wales Summit, decided to strengthen its cyber defences and further engage with Industry; the NATO Communications and Information Agency was assigned this responsibility. Similarly, in July 2016 the EU adopted the first EU-wide legislation on cyber-security in the form of the Directive on Security of Network and Information Systems.

The Master's Degree in "Homeland Security – Systems, Methods and Tools for Security and Crisis Management" of Campus Biomedico University in Rome, is the programme of choice to learn about a country's major security threats, vulnerabilities and risks to CI and to identify and implement adequate safeguards and countermeasures. The programme, which combines theory and real-life cases including in international environments, also illustrates a number of

How does a company or a state actually meet citizens' high expectations for safety, security and business continuity? How can CI be duly protected in order to prevent any damaging incidents, mitigate the consequences when they do happen and allow business to resume as soon as possible? What does "security" mean for a country's CI.

To understand how to manage a crisis before, during and after a so-called

Carlotta Maraschi

is actually Assistant Security Manager at Ferrovie dello Stato Italiane

Anthony Testa

Anthony works at NATO Communications and Information Agency located in Mons, Belgium. He is Head of the Staff Management Office and Chief of the Front Office of his Service Line

A moment of the exercise

"catastrophic event", particularly when it is caused by malicious behaviour, it is necessary to reduce the risks to an acceptable level.

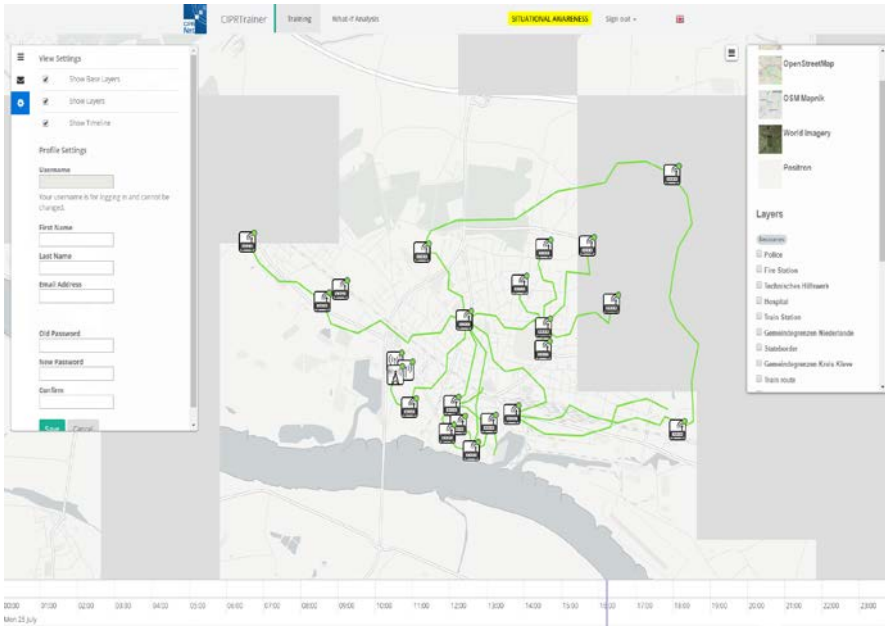
The US federal government has implemented "The Risk Management Process for Federal Facilities: An Interagency Security Committee Standard" which states that "Risk is a function of the values of threat, consequence, and vulnerability. The objective of risk management is to create a level of protection that mitigates vulnerabilities to threats and the potential consequences, thereby reducing risk to an acceptable level".

The CIPRNet what-if analysis tool

One of the highlights of the programme was the two-day seminar organised by the Critical Infrastructure Preparedness and Resilience Research Network (CIPRNet) on how to plan for and manage catastrophic events affecting CI.

It is worth noting that a catastrophic event affecting critical infrastructure (i.e. assets such as energy, transport, telecommunications, health and financial services) together with the management of its consequences may provoke a phenomenon called domino effect, whereby the damages of the attacked infrastructure cause the malfunction of other critical infrastructure, thus negatively affecting other systems and possibly the whole country.

During the CIPRNet seminar we had the chance to experience exactly this: what could be the consequences of poor management following a catastrophic event. The Fraunhofer Institute for Intelligent Analysis and Information Systems IAIS presented a disaster simulator prototype. Through this simulator we were able to analyse the case study regarding an industrial accident in Germany, and a flooding scenario in the Netherlands. We were able to observe the "domino effect" of the decisions taken during the crisis. It was a real eye opener! We could witness how a series of events, poor judgement and ineffective countermeasures could bring the whole operating system of a country to its knees, causing an incredible cascade of costly and damaging delays and inefficiencies.



CIPRNet What-if Analysis tools interface

The relevance of the Human Factor

The availability and efficiency of a country's critical infrastructure is very much dependent on the competence of security experts. In fact, as natural disasters or catastrophic events caused by men can happen any time, it is essential that such security experts maintain high situation awareness, adopt creative and effective solutions and, last but not least, train and exercise regularly. The Master of Homeland Security, Campus Biomedico University in Rome, promotes this approach, provides an excellent way to keep abreast of modern methodologies and tools in the area of protection of CI and combines academic perspectives with pragmatic, real-life experience. It also provides an in-depth assessment of the importance of business continuity planning while defending the reputation of the firm, preserving the morale of the population and strengthening the resilience and resolve of the country.

For more info

See: www.ciprnet.eu

Master in Homeland Security
January-December 2017 – Rome (Italy)
www.MasterHomelandSecurity.eu

Links

ECN home page	www.ciprnet.eu	
ECN registration page	www.ciip-newsletter.org	Please register free of charge
CIPedia©	www.cipedia.eu	the new CIP reference point

Forthcoming conferences and workshops

Master in Homeland Security	www.MasterHomelandSecurity.eu	January 2017

Institutions

Cert of Poland	https://www.cert.pl/en
National and European Information Sharing & Alerting System	www.neisas.eu
European Organisation for Security	www.eos.ecom
Netonets organisation	www.netonets.org

Project home pages

FP7 CIPRNet	www.ciprnet.eu
Criminal use of information Hiding	http://cuing.org
EU DG Home: Cyber-Physical attacks analysis against ICS (FACIES)	http://facies.dia.uniroma3.it
ILLBuster project	http://illbuster-project.eu
International crises exercise in NL	https://english.nctv.nl/current_topics/news/2016/SuccessfulinternationalexerciseVITEX.aspx
Poland Telco Security	https://pl.asseco.com/en/sectors/public-institutions/bipse-security-of-the-teleinformatic-system-374
FP 7 Smart Mature Resilience for Cities (SMR) EU Project	http://smr-project.eu/home
FP 7 SECURity at the network Edge (SECURED)	www.secured-fp7.eu
FP 7 Secures the smart grid of tomorrow	www.segrid.eu
Smart Mature Resilience project	http://smr-project.eu/home
Situation Aware Security Operation Centre (SAWSOC)	http://www.sawsoc.eu
FP 7 Weather CIP risk management and protection	www.intact-project.eu

Interesting Downloads

European Network and Information Security Agency www.ENISA.eu publishes reports and other material on "Resilience of Networks and Services and Critical Information Infrastructure Protection" In this issue e.g.:

ENISA	www.enisa.europa.eu/activities/Resilience-and-CIIP
ICS Certification ENISA	https://resilience.enisa.europa.eu/ics-security
Network Information Security	https://resilience.enisa.europa.eu/nis-platform
Polish National CIP Programme	http://rcb.gov.pl/en/critical-infrastructure/
Platform Current policy debates	http://digitalwatch.giplatform.org
GFCE-MERIDIAN Good Practice Guide on CIIP	https://www.tno.nl/gpciip/

Websites of Contributors

Acris	www.acris.ch
NASK Research Institute of Poland's Ministry of Digitisation	https://www.nask.pl
Campus Bio-Medico di Roma	www.unicampus.it
EC Joint Research Centre	https://ec.europa.eu/jrc
Europol	https://epe.europol.europa.eu
Fraunhofer-Institut für Intelligente Analyse- und Informationssysteme IAIS	www.iais.fraunhofer.de
Wydział Elektroniki i Technik Informacyjnych PW	https://secure.tele.pw.edu.pl
Ministry of Justice Netherland	www.rijksoverheid.nl/ministeries/ministerie-van-veiligheid-en-justitie
TNO	www.tno.nl/en/
Royal Roads Canada	www.royalroads.ca/
United Nations Interregional Crime and Justice Research Institute (UNICRI)	www.unicri.it
Università degli Studi di Napoli Federico II	www.international.unina.it
UNIVERSITA' DEGLI STUDI ROMA TRE	http://uniroma3.it
Uniwersytet Technologiczno – Przyrodniczy	http://utp.edu.pl/en
H2020	http://ec.europa.eu/programmes/horizon2020

www.cipedia.eu

Let's grow CIPedia©

An online community service by the CIPRNet Project.

Derived from the EU FP7 Network of Excellence project **CIPRNet**, CIPedia© aims to be a **Wikipedia-like online community service** that will be a vital component of the CIPRNet's VCCC (Virtual Centre of Competence and expertise in CIP) web portal, to be hosted on the web server of the CIPRNet project.

It is a multinational, multidisciplinary and cross-sector web collaboration tool for information sharing on Critical Infrastructure (CI)-related matters. It promotes communication between CIP-related stakeholders, including policy-makers, competent authorities, CI operators and owners, manufacturers, CIP-related facilities and laboratories, and the public at large.

> Within two years, CIPedia© reached 440,000 total views, at a current average of 450 views per day.

CIP terminology varies significantly due to contextual or sector differences, which combined with the lack of standardisation, create an unclear landscape of concepts and terms. CIPedia© tries to serve as a point of **disambiguation** where various meanings and definitions are listed, together with additional information to relevant sources.

In its current stage of development, CIPedia© is a collection of pages – one page for each **concept** with key **definitions** from various sources. It is supplemented by: a list of CIP **conferences**, several sector-specific **glossaries**, CIP-related **bibliography**.

> Your contribution is essential for putting value in the CIPedia© effort.

In future stages it will include discussion topics on each concept, links to useful information, important references, disambiguation notes, and more. The full articles will eventually grow into a form very different from dictionary entries and related concepts can be combined in one page. CIPedia© does not try to reach consensus about which term or which definition is optimum, but it records any differences in opinion or approach.

The CIPedia© service aims to establish itself as a **common reference point for CIP concepts and definitions**. It gathers information from various CIP-related sources and combines them in order to collect and present knowledge on the CIP knowledge domain.

Marianthi Theocharidou

Marianthi Theocharidou is a Research Fellow at the European Commission's DG Joint Research Centre (JRC), working for the CIPRNet, IMPROVER and ERNCIP projects.

marianthi.theocharidou@jrc.ec.europa.eu

Expression of Interest

CIPedia© now welcomes **CIP experts** to actively **contribute**:

- ✓ Add definitions and references!
- ✓ Create a new topic!
- ✓ Start a discussion!
- ✓ Moderate!

If you are interested to become an active contributor, please contact Dr. Theocharidou for information.