European CIIP Newsletter

March - June 2017, Volume 11, Number 1

Industrial Control System (ICS) Security Focus

ECN

Contents

Editorial

EU & Int. Projects: CIPRNet, FIRST, TACIT PRE-DICT, CIRCLE

CIIP Good Practice Guide \ Democrite FR

ICS Protection, L2 Sec in CIP, CI Tools Testing, Zero-Day Defence
iHoneypot
CRITIS 2016 & 2017

Upcoming Conferences and Links

CIPedia@

> 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

> Spelling:
British English is used except for US contributions

Editorial

Editorial	Towards a European Infrastructure Simulation and Analysis Centre (2E!SAC), CIPRNet Completed by Javier Lopez and Bernhard M. Hämmerli	5

European and Global Activities

CIPRNet EU Project	CIP/CIR Community Services offered by CIPRNet's Virtual Centre of Competence & Expertise in CIP by Erich Rome, Eric, Luiijf and Vittorio Rosato	7
First & Incident Response	Energy sector and incident response by Margrete Raaum	11
TACIT EU FP7	Cyber Threat Simulation in Smart Grids: The TACIT solution by Erkuden Rios	13
PREDICT EU FP7	Spatial-aware Iterative Integration of Crisis Management Information Systems by Jingquan Xie and Betim Sojeva	17
CIRCLE EU FP7	CIRCLE: Pan-European framework for strengthening Critical Infrastructure resilience to climate change by Athanasios Sfetsos	19
GFCE-Meridian	A Good Practice Guide on Critical Information Infrastructure Protection by Eric Luiijf and Tom van Schie	21

Country Specific Issues

France CYCA Co-Winner	Human vulnerability mapping facing critical service disruptions for crisis management by Amélie Grangeat	23

Method and Models

ICS Protection	Protecting Industry 4.0 against Advanced Persistent Threats by Javier Lopez	27
CYCA Co-Winner	Effective Defence against Zero-day Exploits Using Bayesian Networks by Tingting Li	31

Method and Models

L2 Sec in CIP	Ensuring Network Security for Critical Information Infrastructures by Christoph Jaggi	35
CI Tools Testing	A taxonomy of tools for CI Security Testing by Marina Egea et. Al.	39
iHoney far ICS	iHoney Project: New concepts in honeypot development for ICS cybersecurity by Oscar Navarro	43
CRITIS 2016	CRITIS 2016: Conference Highlights by Grigore M. Havârneanu	47

Ads of upcoming Conferences and Workshops

YCA	Young CRITIS Award	6
Cascading Effect Conferences	Joint final conference of „cascading“-projects CASCEFF, CIPRNet, FORTRESS, PREDICT, SNOWBALL	10
IFIP 2017	International Conference on Critical Infrastructure Protection	26
52nd ESReDA	Seminar On Critical Infrastructures: Enhancing Preparedness & Resilience for the security of citizens and services supply continuity	30
CRITIS 2017	CRITIS 2017: 12th International Conference on Critical Information Infrastructures Security – CFP by Antonio Scala and Gregorio D'Agostino	49
CRITIS 2017 Ad	Joining CRITIS 2017 In Lucca	52

Links

Where to find:	Forthcoming conferences and workshops / Recent conferences and workshops / Exhibitions / Project Selected download material	53

Media on C(I)IP

CIPedia©	Let's grow CIPedia© by Marianthi Theocharidou	54

Towards a European Infrastructure Simulation and Analysis Centre (2E!SAC), CIPRNet Completed

Looking back to our mission with CIPRNet and inspiring with some thoughts for the future

CIPRNet project ends February 28, 2017, a good opportunity to look back at how it started: In 2010 at the Centre for European Policy studies, I chaired the taskforce "Critical Infrastructure Protection in the EU". CIPRNet coordinator Erich Rome, whom I knew from being a part of the EU project "Integrated Risk Reduction of Information-based Infrastructure Systems" www.irriis.org, was invited to a session for postulating a European Infrastructure Simulation and Analysis Centre in analogy to the NISAC in the USA. This vision still connects us with many other friends, which would like to see Europe taking more responsibility in this direction.

Erich Rome guided our CIPRNet team with superior seniority and reached significant advances by implementing the vision of the network of excellence CIPRNet: new capabilities for CIP stakeholders, dissemination and training activities that made CIPRNet highly visible in the communities, and a high degree of integration amongst partners. The team is now an interlinked network of friends pushing the resilience of vital infrastructure resilience in the EU. The recently founded association for fostering vital infrastructure resilience in Europe (2E!SAC) shall sustain the promotion of EISAC and we hope for further advances. Each one of us feels, that times are changing and we need more in-depth knowledge of our infrastructure and prediction how the CI behaviour and disaster consequences would be assuming different scenarios. CIPRNet could deliver two new applications built on top of earlier proofs of concept: advanced decision support and 'what if' analysis for exploring different courses of crisis management actions.

The consequent promotion of the CRITIS topic in the young scientist community, including them also in the boards of the conference developed its fruits. The last competition of the CIPRNet Young CRITIS Award (CYCA) in Paris had 17 registration of researchers below 32 years. This promotion will continue as Young CRITIS Award (YCA) at the 12th CRITIS Conference in Lucca, Italy. Somewhat less obvious was the work we did with respect to gender balance. Although our community is still dominated by men, a considerable number of women from different European countries were invited to contribute to the success of CIPRNet: not only as researches but also as keynote speakers, chairs to CRITIS conferences and members of CIPRNet's International Advisory Board. The CYCA competition had two male and two female winners, the ideal balance. And finally, the ECN contributions came out gender balanced in a natural way. We consider such balancing strategies an important element of capacity building, which will make our community richer and more powerful in the long run.

Looking into the future our challenge for resilient infrastructure will most likely grow: The upcoming digitization using the Internet of Things and connecting SCADA and ICS to the Net are pending issues with a lot of research needs. We are proud that CYCA co-winner TingTing Li shares her work in this issue. Also in this issue is a large share of articles developing the SCADA / ICS challenge: society's most essential systems are vulnerable and protection is not completely feasible. This means that we have to develop resilience, which fine-tunes the three domains protection, detection and reaction in a balanced way. Raising reaction, crisis management is a central part of reaction, and we are proud on Amélie Grangeat the CYCA co-winner 2016 presenting results for this domain.

In general, all Member States are somehow short on money and have limited political will to invest a lot into infrastructure. More security would mean higher costs, which turns into higher infrastructure usage fees: a message, which is difficult to sell, and impossible to win elections. As professors we know that motivations for learning are simplistic: avoiding pain, gaining advantage and very seldom intrinsic joy. But mostly we learn through pain. In case of CRITICAL

Continued next page ...

Javier Lopez

Prof. Javier Lopez is Full Professor in the Computer Science Department at the University of Malaga, and Head of the NICS Lab. He is Co-Editor in Chief of IJIS journal and the Spanish representative in the IFIP TC-11 on Security and Privacy Protection in Information Systems.

e-mail: jlm@lcc.uma.es

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

Infrastructure this means painful outages and failures that produces sufficient power to change the conditions towards more resilience. In between we focus on little incremental steps and work on a readiness with experts, ideas, concepts to be ready, when more engagement is wanted.
Please look at six focus topics of **12th edition of the CRITIS conference** in October 2017 in Lucca, Italy. Please prepare your submissions no later than June 5 for submission. see: www.critis2017.org.

We thank Javier Lopez, co-editor for his brilliant support for this issue and for all his engagement within CRITIS Conference Series.

We thank all contributors of the newsletter, of projects related to CIP and Crises Management for their work and their contributions, especially those who wrote in the ECN.

Enjoy reading this issue of ECN!

Bernhard M. Hämmerli on behalf of CIPRNet work package ECN

CRITIS 2017

12th International Conference on
Critical Information Infrastructures Security
October 9–13, 2016, Lucca, Italy

Call for Paper open until June 2nd, 2017, see

www.critis2017.org

Young CRITIS Award

www.critis2017.org/young-critis-award

If you are less than 32 years and you contribute,
You may win extra money: Please apply!

CIP/CIR Community Services offered by CIPRNet's Virtual Centre of Competence & Expertise in CIP

The CIPRNet project has established a Virtual Centre of Competence & Expertise in Critical Infrastructure Protection, offering a variety of services to the multi-community of stakeholders and researchers in Critical Infrastructure Protection and Resilience (CIP/CIR).

The EU FP7 Network of Excellence project CIPRNet has bundled its services to the CIP/CIR community in a Virtual Centre of Competence & Expertise in CIP (VCCC). The VCCC services include CIP/CIR knowledge sharing, demonstrations of new technical capabilities, an e-Learning platform, and access to CIPedia©, a very popular online glossary of CIP/CIR terms. The VCCC services can be accessed via CIPRNet's website. Moreover, most of the VCCC services will be kept active beyond the end of CIPRNet.

One of the major objectives of CIPRNet was to lay the foundation for a long-lasting centre of competence and expertise in Critical Infrastructure Protection (CIP), the ***European Infrastructures Simulation & Analysis Centre*** (**EISAC**). The CIPRNet consortium knew that implementing EISAC is a process that would take longer than the project's lifetime. Therefore, CIPRNet planned starting this process by creating the VCCC during the project term.

Many of CIPRNet's activities in research and technological development (RTD), training, and dissemination resulted in service offerings. These offerings are tailored to CIPRNet's audience: CI operators, CIP/-CIR policy-makers, and R&D community [1]. In this article, we describe which services are provided by the VCCC.

Service groups

CIPRNet uses a service framework consisting of a set of service groups for describing the VCCC's offerings to the CIP/CIR community. VCCC services include training and dissemination activities, web-based repositories (like a database of CIP related research projects), facilities like CIPedia©, and demonstration services of CIPRNet's new capabilities.

Service group Advanced Decision Support

This service group refers to the two new technological capabilities that CIPRNet has produced:

- **CIPCast**, a **Decision Support System**, aimed at supporting CI operators and civil protection agencies [2][5][9].
- **CIPRTrainer**, a training system that enables performing **'what if' analysis** in complex simulated crisis scenarios for exploring different courses of action and using consequence analysis [6][7]. Its target audience are crisis managers at the operational-tactical level of civil protection.

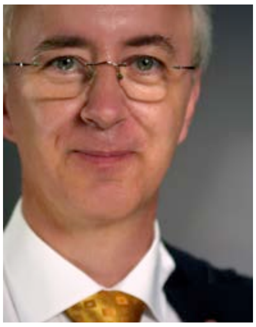
> Aiming at a sustained operation of the VCCC, CIPRNet members will keep most of the services active beyond the end of the project.

Capability related services that remain active beyond CIPRNet are the web demonstration services of CIPRTrainer (Figure 1) and CIPCast (Figure 3), both accessible via the VCCC web portal: http://www.ciprnet.eu/315.html

Service group Training

This group of services comprised training events such as CIPRNet courses, Master Classes, and lectures offered during the term of CIPRNet.

CIPRNet has issued a textbook [4] on the training material developed for the training events.



Erich Rome

...is a senior researcher at Fraunhofer IAIS and the coordinator of CIPRNet.

e-mail: erich.rome@iais.fraunhofer.de

Eric Luiijf

...is principal consultant at the Netherlands Organisation for Applied Scientific Research TNO and an expert in C(I)IP. He leads the VCCC activities.

e-mail: eric.luiijf@tno.nl

Vittorio Rosato

...is head of the Analysis and Protection of Critical Infrastructures Lab at the ENEA Casaccia Research Centre. ENEA provides several VCCC services.

e-mail: vittorio.rosato@enea.it

A web service that remains active beyond CIPRNet is its MOOC (Massive Open Online Courses) CIP/CIR e-learning courseware. It contains parts of the CIPRNet training material, video recorded lectures, and sets of multiple-choice questions. The MOOC platform is directly accessible via this URL:
http://www.security-learning.eu

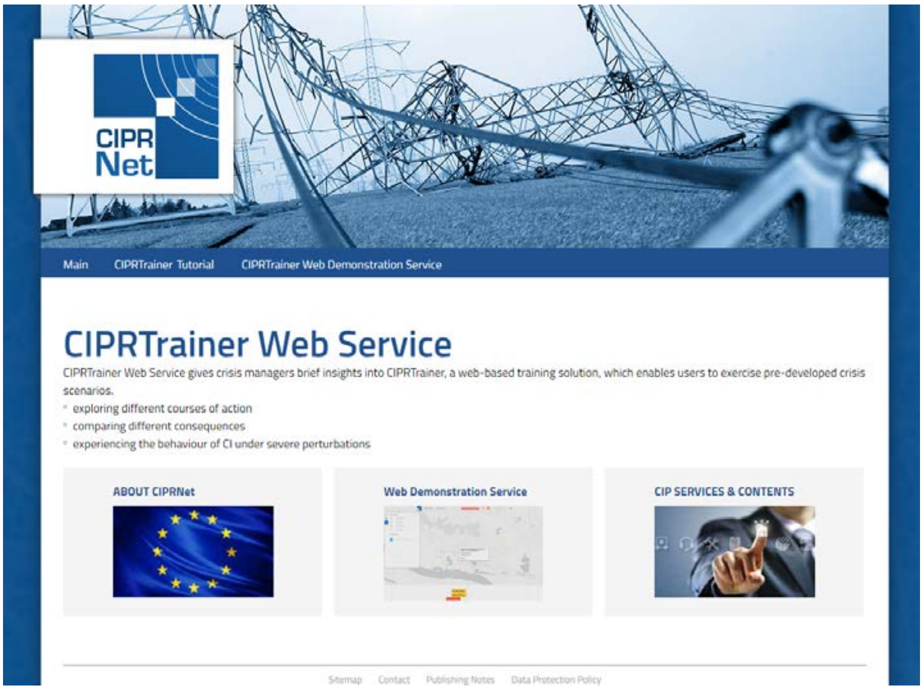
Service group Information Brokerage on CIP/CIR

This service group refers to glossaries, repositories, and databases related to CIP/CIR that are offered as CIP/CIR community services. Accessible services are:

- "Ask the Expert"
- CIPedia©.

"Ask the Expert" [8] is a knowledge brokering service. Users may use the web-based service for asking CIP related questions. Registered (CIPRNet) experts whose area of expertise matches the question are automatically asked to answer the question.

CIPedia© is probably one of the two most successful outcomes of CIPRNet. This Wikipedia-like online glossary of CIP/CIR related terms and definitions has received about half a million views with a daily average of about 475 views. CIPRNet partners made a massive effort for making CIPedia© address the international dimension of CIP/CIR by adding definitions from almost 100 different nations and in more than 40 different languages. This community service will sustain, kept alive by a multi-disciplinary community. Besides CIPRNet, the EU H2020 project RESIN (resin-cities.eu) has made contributions to CIPedia©.
The link to CIPedia© is also included in the VCCC web portal services page. CIPedia© is directly accessible via:
http://www.cipedia.eu



CIPRTrainer Web Service

CIPRTrainer Web Service gives crisis managers brief insights into CIPRTrainer, a web-based training solution, which enables users to exercise pre-developed crisis scenarios.

- exploring different courses of action
- comparing different consequences
- experiencing the behaviour of CI under severe perturbations

ABOUT CIPRNet

Web Demonstration Service

CIP SERVICES & CONTENTS

Figure 1: CIPRTrainer web demonstration services.

Service group Research Platform for CIP/CIR Collaboration

This service group bundles CIPRNet repositories and activities related to research and technological development (RTD). **Repositories** accessible via the VCCC web portal Research Platform include:

- a CIP EU **research project list**,
- a CIP/CIR **bibliography**, and
- an initial CIP MS&A **benchmark reference set**.

The latter contains a full scenario containing artificial CI data and threat models, including dependencies and cascading relationships. It is meant as a benchmark reference set for CIP Modelling, Simulation & Analysis (MS&A).
The elements of this service group are directly accessible via the VCCC web portal:
http://www.ciprnet.eu/315.html

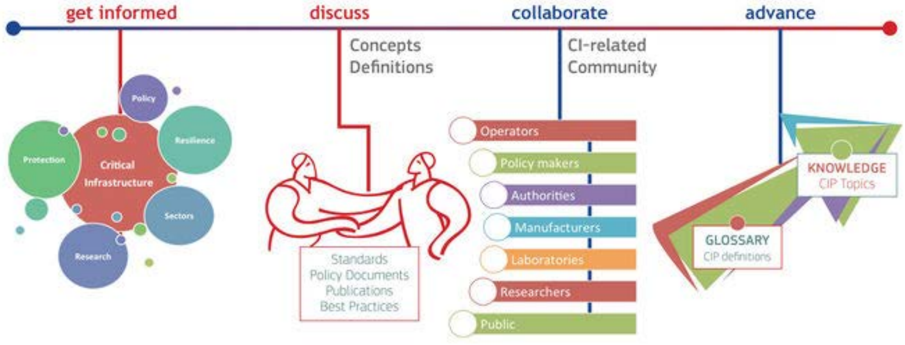


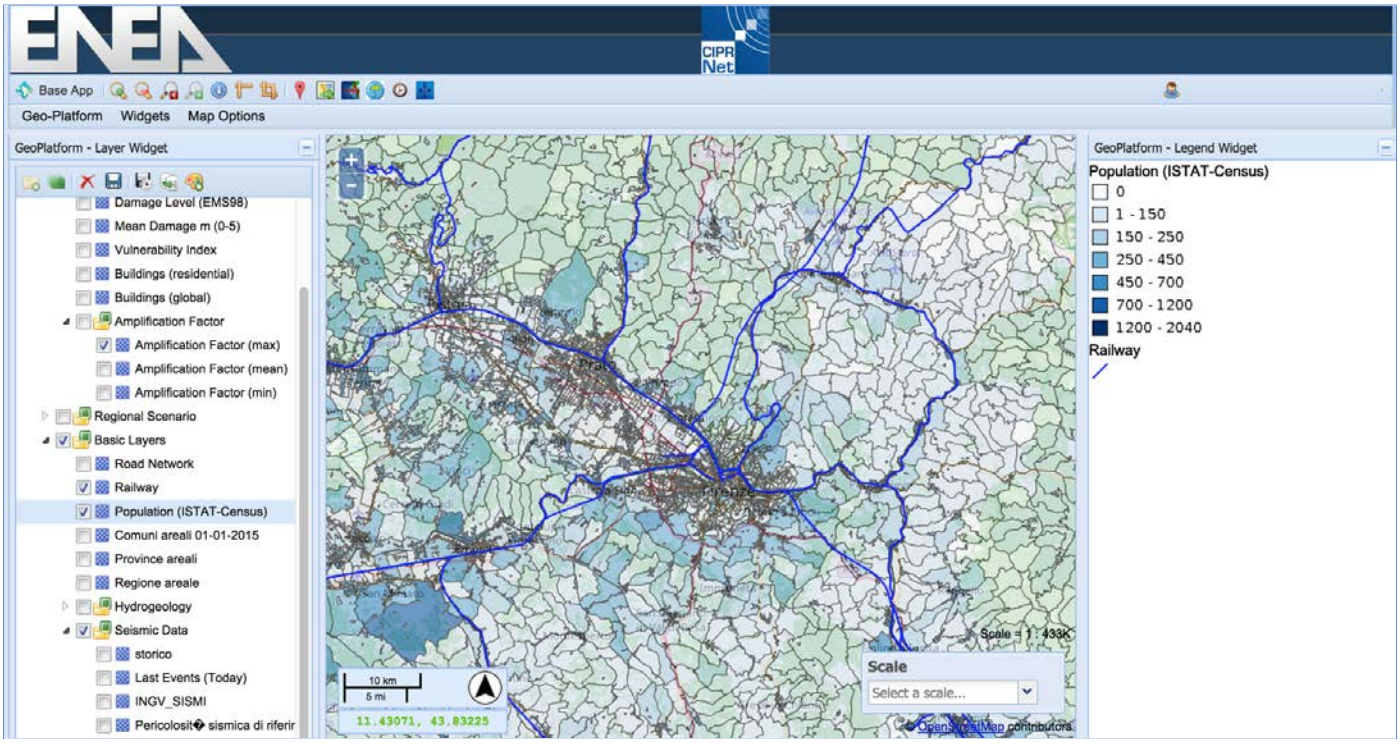
Figure 2: CIPedia© as a community service

Service group Dissemination

This group of services comprises the support of CIP/CIR related **conferences** like CRITIS, netonets, TIEMS, and the ESReDA seminars (see "More Information" at the end of this article), the **European CIIP Newsletter ECN**, the CIPRNet **publications**, the CIPRNet **deliverables**, and a **list of CIP/CIR conferences** on CIPedia©.
After the end of CIPRNet, CIPRNet's public pages on publications and deliverables will go into archival status. The links to these pages are:
https://www.ciprnet.eu/refereed-publications.html
https://www.ciprnet.eu/deliverables.html
CIPRNet partners will remain active in supporting CIP/CIR related conferences. The continuation of the ECN depends on the availability of continued funding (sponsors are welcome!). Visit the ECN (European CIIP Newsletter) home page, which includes an archive of all previous issues:
http://ciprnet.eu/ecn.html

Conclusion and Outlook

The VCCC is the end-result of CIPRNet in terms of services. Some of the established CIPRNet services, hosted by different partners, will be maintained and continued after the end of the CIPRNet project. Other advancements will not be maintained lacking time and funding; these will be made



□ Damage Level (EMS98)
□ Mean Damage m (0-5)
□ Vulnerability Index
□ Buildings (residential)
□ Buildings (global)
□ Amplification Factor
☑ Amplification Factor (max)
□ Amplification Factor (mean)
□ Amplification Factor (min)
□ Regional Scenario
☑ Basic Layers
□ Road Network
☑ Railway
☑ Population (ISTAT-Census)
□ Comuni areali 01-01-2015
□ Province areali
□ Regione areale
□ Hydrogeology
☑ Seismic Data
□ storico
□ Last Events (Today)
□ INGV_SISMI
□ Pericolosit� sismica di riferir

Population (ISTAT-Census)
- 0
- 1 - 150
- 150 - 250
- 250 - 450
- 450 - 700
- 700 - 1200
- 1200 - 2040

Railway

Figure 3: Screenshot of CIPCast-IT, a web service demonstrating the new capability of advanced decision support for coping with CI related emergencies and disasters

visible in the VCCC's CIPRNet archive section. Several CIPRNet members and one external partner founded the German association 2E!SAC ("Verein" – association with international members by German law) to have a formal frame for continuing the CIP/CIR activities and services towards establishing and sustaining CIP/CIR competence centres in several European nations and at the EU level. Enquiries regarding this association could be sent to the authors of this article. Check out the VCCC services, contribute to CIPedia©, and let us know your ideas.

References

[1] Kozik R., Choras M., Flizikowski A., Theocharidou M., Rosato V., Rome E., "Advanced services for critical infrastructures protection". Journal of Ambient Intelligence and Humanized Computing, Springer Berlin Heidelberg, ISSN 1868-5137, December 2015, Volume 6, Issue 6, p. 783-795, http://dx.doi.org/10.1007/s12652-015-0283-x.

[2] Di Pietro A., La Porta L., Pollino M., Rosato V., Tofani A., Martí J.R., Romani C., "A Decision Support System for Emergency Management of Critical Infrastructures subjected to Natural Hazards," in conference proceedings Critical Information Infrastructures Security,

[3] 9th International Workshop (CRITIS2014), Berlin, LNCS vol. 8985, Springer, Heidelberg, 2016, pp. 362-367.

[4] Setola R., Rosato V., Kyriakides E., Rome E. (Eds.), "Managing the Complexity of Critical Infrastructures: A Modelling and Simulation Approach", Series: Studies in Systems, Decision and Control, Vol. 90, Springer, ISBN 978-3-319-51042-2, 2017.

[5] Di Pietro A., Lavalle L., La Porta L., Pollino M., Tofani A., Rosato, V., "Design of DSS for Supporting Preparedness to and Management of Anomalous Situations in Complex Scenarios". In: [4]

[6] Rome E., Doll Th., Rilling S., Sojeva B., Voß N., Xie J., "The Use of What-If Analysis to Improve the Management of Crisis Situations". In: **Fehler! Verweisquelle konnte nicht gefunden werden.**

[7] Rome E., Xie J., Sojeva, B.: "CIPRTrainer – simulation-based »what if« analysis for exploring different courses of action in crisis management." ECN 24 (vol 10, no 2), 2016.

[8] The CIPRNet Team: "ATE: A virtual Competence Centre in Critical Infrastructure Preparedness and Resilience." ECN 23 (vol 10, no 1), 2016.

[9] Tofani A., De Nicola A., Di Pietro A., Pollino M., La Porta L.: "Data management and Information sharing in CIPRNet DSS." ECN 19 (vol 8, no 2), 2014.

Disclaimer and Acknowledgement

The project CIPRNet has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 312450.

The contents of this publication do not reflect the official opinion of the European Union. Responsibility for the information and views expressed herein lies entirely with the authors.

The authors gratefully acknowledge the contributions of the entire CIPRNet project team!

More information

If you would like to find out more about the CIPRNet project, then please visit the project's website at

http://www.ciprnet.eu

and check the "Services" page.

Check out CIPedia©, CIPRNet's popular online glossary of CIP related terms at

http://www.cipedia.eu

Visit the ECN (European CIIP Newsletter) home page, which includes an archive of all previous issues: http://ciprnet.eu/ecn.html

Links to conference and seminars supported by CIPRNet

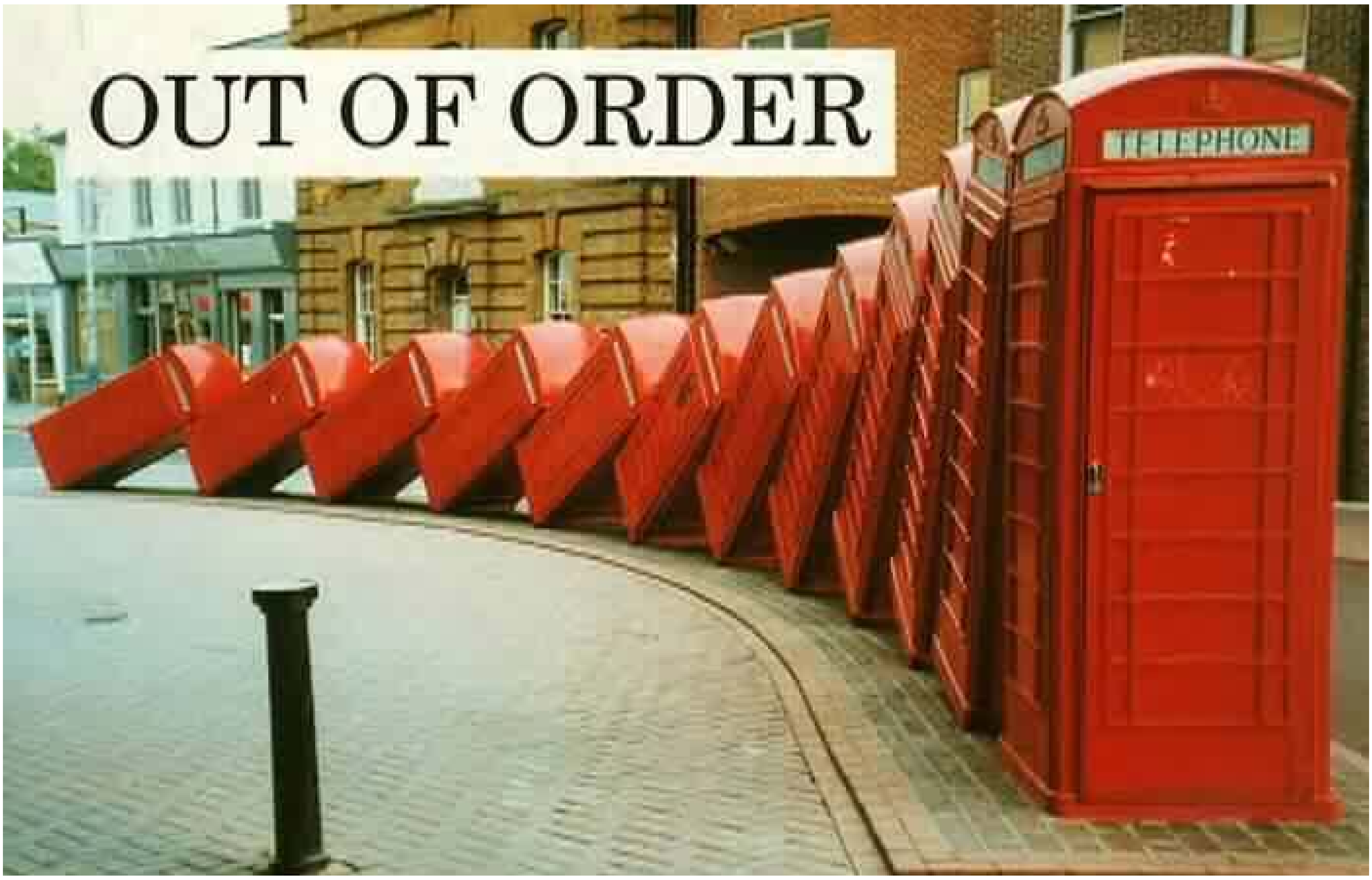
CRITIS	http://www.critis2016.org
netonets	http://www.netonets.org
TIEMS	http://tiems.info

Joint final conference of projects on cascading CI Effects

CASCEFF, CIPRNet, FORTRESS, PREDICT, SNOWBALL

March 16, from 13:30h and March 17, 2017

Brussels, BAO, le Bouche à oreille, Rue Félix Hap, 11, 1040 Brussels



The **joint final conference** will place on the **16th of March** 2017 (afternoon) and in all day **17th of March** 2017 (1,5 days).

see

www.cascadingeffects.eu

Energy sector and incident response

As the attack surface increases and attackers are becoming increasingly aware of the possibilities in attacking the energy sector, the sector must prepare to respond to cyber incidents and to share not only data on incidents, but also knowledge.

Introduction

Most of the critical infrastructure is going through a digital revolution, as automation is opening new doors to safer and more efficient infrastructure, as well as doors to new possibilities and effects in old industries. The industrial control systems (ICS), enables the operators in for instance the energy sector to ensure the frequency and balance are at the right levels at all times, and controlling this centrally gives a comprehensive view of the system, enabling better administration.

Unfortunately, the industrial control systems were not created with security features, hence as the industry becomes increasingly connected, the number of possible attack vectors increase. The new generation control systems are built with common off-the-shelf components, which on the one hand opens up for security functions like logging, white-listing and anomaly detection. On the other hand, the operating systems will, to a larger extent, be known and widely available to the attacker.

The number of published vulnerabilities in ICS is rising, because more and more vendors are either security testing their products or are more or less willingly being tested by security researchers. This has two sides. On the one hand the control system elements are finally being tested, but on the other hand the number of zero-days in control systems available to attackers will rise too (see figure 1).

With "smart meters" in all homes, and a legitimate desire to extract useful data to improve both new and old services, the industry is opening a door to a wider range of threats than most are prepared to meet. The maturity in digital security operations and incident response is still alarmingly low.

Attackers Enterprise Model

The attackers we face may be advanced or even just well-coordinated, but we also frequently see that attackers stumble across industrial control systems because they are too readily available. Today's threat picture is complex, and the older model with hacktivists vs. criminals, spies or nation state does not cover today's situation. It has become a many-tiered, distributed, enterprise model. In this model, you can find small time hackers that sell breached accounts or social engineering results, researchers that find and sell zero-day vulnerabilities in ICS, programmers that specialise in utilising these vulnerabilities to create an "attack software", others that specialise in software designed to download the "attack software".

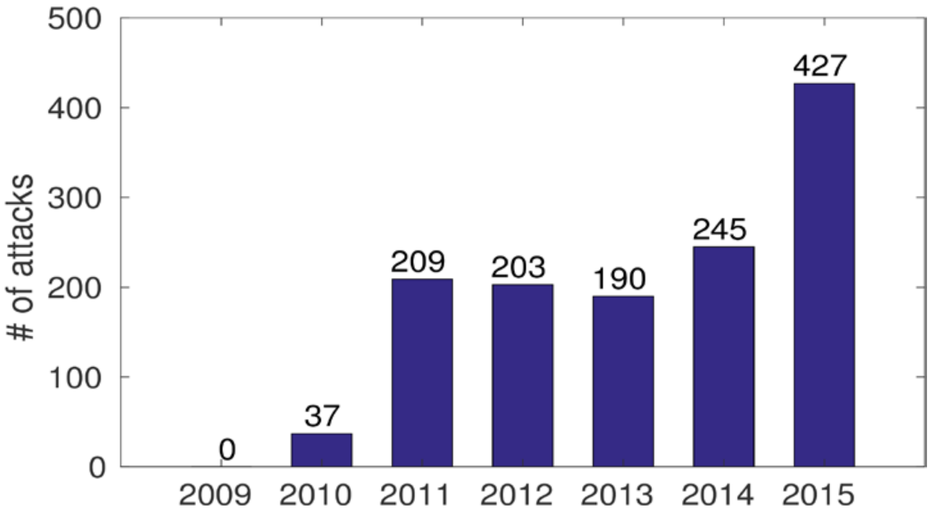


Figure 1: Vulnerabilities published through the ICS-CERT from 2009 - 2015

Margrete Raaum

has worked in information security since 1998, and later in incident response in academia where she started UiO-CERT, at the national CERT, NorCERT, and with the Norwegian TSO, Statnett. She wrote a master thesis on trust in information sharing networks in 2012 at HiG/NTNU. She is Chairman of the board of directors of FIRST (Forum of Incident Response and Security Teams), and CEO and team leader for KraftCERT, the Norwegian energy sector incident response team.

e-mail: margrete.raaum@first.org

www.first.org
www.kraftcert.no/english

The attacker utilising the tools does not have to be, and seldom is, a developer, and the parties ordering the attack may be anyone with no technical knowledge, just a desire to stage an attack. The world's attention is now on the energy sector and the control systems, especially after the Ukraine attacks, and the amount of damage that can be done is unfathomable. We need to look at the challenges ahead and apply appropriate measures.

Most industries have the basic passive defences like firewalls and anti-virus in place, but are relying too much on these defences. Several security experts in the energy sector talk about the dangers of relying on these passive perimeter defences, but are still caught off guard when attackers or malware pass these defences. Which is the last thing that should happen to the defenders of critical infrastructure: to be caught off guard.

The traditional defences are failing. Avoiding detection in firewalls is trivial, and even if signature based intrusion detection mechanisms are not a reliable defines alone, some are not even there yet. Before we can move on to active detection and defines, we need to have a sound architecture with a zone model and proper inventory in place. You cannot protect what you do not know you have. If you are in full control of inventory and traffic flows, it is possible to baseline traffic and equipment configurations, which is a much more powerful anomaly detection than a mainstream solution.

Passive defines is still worth something, but active defines reflects a cyber security maturity that prevents real damage. (see fig 2)

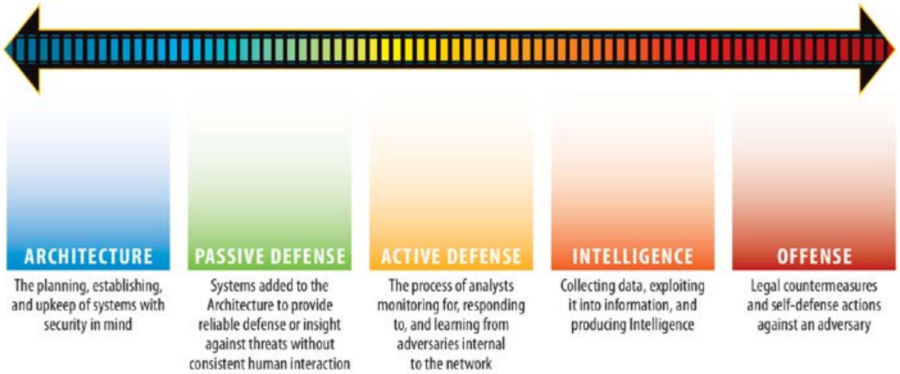

ARCHITECTURE
The planning, establishing, and upkeep of systems with security in mind
PASSIVE DEFENSE
Systems added to the Architecture to provide reliable defense or insight against threats without consistent human interaction
ACTIVE DEFENSE
The process of analysts monitoring for, responding to, and learning from adversaries internal to the network
INTELLIGENCE
Collecting data, exploiting it into information, and producing Intelligence
OFFENSE
Legal countermeasures and self-defense actions against an adversary

Figure 2: The SANS sliding scale of cyber security by Robert M. Lee

Preparing for Breaches

Everybody must prepare for a breach, therefore we all need dedicated cyber incident response team. It can be argued that there is an advantage having sector based incident response teams: In a single sector the technology, the external threats and the vulnerabilities will be similar. Also, there is a common culture and even personal relationships so there will be a high level of trust. A high level of trust is crucial to be able to promote the sharing of incident information. If the reporting is forced, and not trust based, the sharing parties will likely not share more than is absolutely necessary.

> „Everybody must prepare for a breach: –
> this is why we need dedicated incident response teams"

When choosing the initial constituency for KraftCERT, the Norwegian Energy Sector CERT, these considerations were made. Also, a team serving the energy sector should have insight into ICS, ideally also into the local systems, and this requires a close relationship with absolute trust. Being able to see the specific needs of each constituent is important to be able to choose the most important focus areas for advisories and guidelines. The voluntary membership and sharing model does also seem to work, however, as predicted in *Flammini et al. [1]*, the amount of data is low when the general activity is low. We are currently working with the larger actors, under the assumption that if major actors start sharing, the activity level will rise.

The lack of political involvement has been a critical success factor, as the focus has been on close communication, high trust level and of identifying both the individual Achilles' heels and possible areas of cooperation. We have observed that in some sectors and countries, the creation of sector incident response teams or ISACs (Information Sharing and Analysis Centre) have turned into a political battle, and this is time wasted that should be spent building up capacity.

A crucial task for a sector incident response team is to keep updated on the threat picture. This requires tight connections to other teams in other countries. KraftCERT became a full member of Forum of Incident Response Teams (FIRST) in 2016 to enable sharing of threat intelligence and attack details with other teams worldwide.

International information sharing

FIRST (www.first.org) is an international umbrella organisation that brings together trusted computer incident security teams from around the world, from all sectors. Membership enables incident response security teams to handle security incidents more effectively and to better prepare for future attacks, and 369 teams from 76 countries participate in FIRST. The members develop and share technical information, tools, methodologies, processes and best practices, and helps nations all over the globe build national incident response teams. Within the organisation, there are special interest groups (SIGs) that bring people together in more tightly knit collaboration, e.g. the Special Interest Group for Industrial Control systems.

We must try to keep up with the threat picture and the adversaries together, and the key to this is information sharing and trust. We need to share, not only incident data, but tools and tricks of the trade. Not everybody should have to invent the wheel, and there should be trust enough to be able to share both strengths and weaknesses. We should take the time to assist others in securing their infrastructure by sharing our findings with the community. Offering information and tools without being explicitly asked is also a way to show the community what other actors in critical infrastructure are working on.

[1] *Effective Surveillance for Homeland Security: Balancing Technology and Social Issues. Chapter 2: Trust networks among human beings by Hämmerli et al.*

Cyber Threat Simulation in Smart Grids: The TACIT solution

A smart approach to cybersecurity protection in critical infrastructures includes threat simulation for design validation and operator education.

Cyber threats in Smart Grids

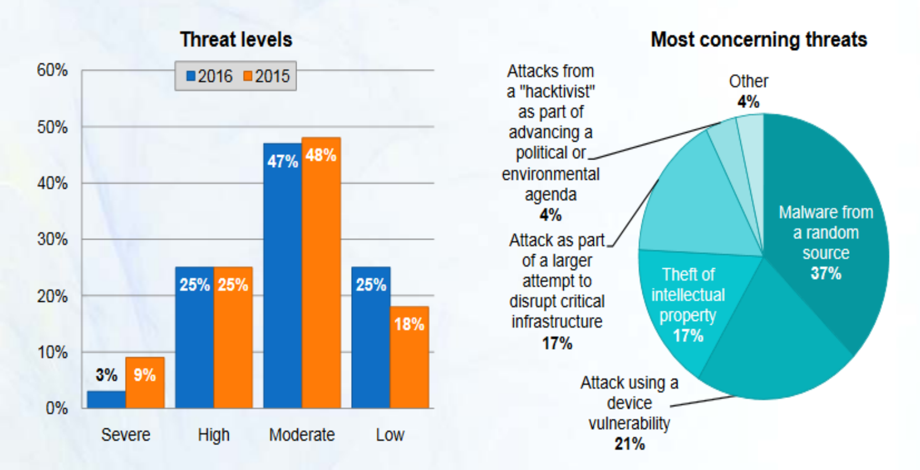
The digital transformation of the energy systems within EU is described in detail in the Digital Energy System 4.0 report by the European Technology Platform for Smart Grids [1].

As Smart Grids become more sophisticated and dependent on ICT systems, the exposure surface increases and threats diversify. According to ENISA [2][3], the Smart Grid threats can be classified by their intentional vs. accidental/inadvertent nature, and other detailed classifications may be made considering the target of attack, attack techniques used, etc.

Below is a classification of main threats over electricity grids identified by the EU-funded TACIT research project [4]:

- *Threats related to Smart Grid components and devices* in order to retrieve sensible data from them or interrupt (or hamper) their functioning, i.e. Denial of Service (DoS) attacks, which could make critical resources unavailable.
- *Device or system errors* caused by malfunctions or misconfigurations.
- *Component or device manipulation*, either software or hardware based (including changed behaviour, disabled functions or enabling remote backdoors, malware infection, etc.).
- *Unsafe communication networks and protocols*. Even if in the last years many efforts to secure the protocols used are being made, still some unsafe ones remain.
- *Unauthorised data leakage or distribution*. An attack where critical or technical data regarding a Smart Grid is made public could give place to further attacks based on such information.
- *Human factor threats* that include: i) external attacks that exploit social engineering techniques to harvest employee data or sensitive information, eventually targeting to gain access to internal resources, ii) insider attacks mainly from discontent employees, and iii) unintentional attacks due to the use of not sanitised own equipment and BYOD.
- *Physical threats* including sabotage, theft (device, media), fraud by physically acting on the device, etc.

The Cyber Security survey conducted by control Engineering [5] showed results on perceived threats on industrial control systems. A total of 72% of respondents considered their control system cyber security threat level to be low to moderate, and 37% are most concerned about malware threats coming from a random source.



Q: What level do you perceive the control system cyber security threat within your organization to be? (n=220;278); Q: What type of threat to your control system concerns you the most? (n=223)

Figure 5: Threats in control systems. Source: Cyber Security May 2016 by Control Engineering

Erkuden Rios

is R&D project manager in the ICT Division of Tecnalia. She is currently coordinator of the H2020 project on multi-cloud security (MUSA) [14], and the coordinator of the Data Protection, Security and Privacy in Cloud EuroCloudCluster of EU-funded projects, launched by DG-CNECT in April 2015 [15]

She is specialised in trust and security engineering technologies and has worked in a number of large European and Spanish national projects on the subject such as TACIT, RISC, ANIKETOS, SWEPT, CIPHER and SHIELDS. Erkuden collaborates with Technology Platforms and Forums such as ECSO and the Spanish Technology Platform on Trust & Security – eSEC.

After obtaining her MSc in Telecommunication Engineering at the University of Basque Country (Spain), she worked for Ericsson Spain for 6 years before joining Tecnalia in 2003.

e-mail: erkuden.rios@tecnalia.com

The TACIT solution

The TACIT solution was born within TACIT EU-funded research project, *Threat Assessment framework for Critical Infrastructures protection* [4], oriented to enhance the security of Smart Grids. The main objective of TACIT is the definition and development of a framework for the assessment of risk and impact of cyber-attacks in Smart Grids.
Four European companies participated in the project:

Fundación Tecnalia Research & Innovation (Spain) is a private, non-profit, applied research centre with strong market orientation through the innovation and technological development.

Everis Aerospace and Defense (Spain) is a division of Everis group that provides solutions for critical systems in aerospace, space, defence, security and emergency sectors.

D'Appolonia (Italy) is a large private engineering consulting company with European relevance, really focused on critical sectors in the market.

The Industrial Cybersecurity Center (Spain) is one of the main independent organisations for cybersecurity in Critical Infrastructures with relevance worldwide (Europe, South Arabia, etc).

> The TACIT solution is a Cyber Threat Simulator that enables to simulate and visualise the impact of cyber-attacks in electricity Smart Grids.

The TACIT project developed a proof of concept of a risk assessment framework for Smart Grids that was validated through a series of test cyber-attacks' simulations that led derive appropriate recommendations to enhance cyber security in Smart Grids.

To this aim the project developed a Smart Grid Simulator able to simulate how existent and recently discovered cyber-attacks are spread through actual end-user Smart Grid networks. The simulator allows for identifying the security issues and risks over different elements of the Smart Grid and helps estimating the associated impact.

Threats simulation

Threat simulation usually relies on a well-structured threat specification or modelling for the systematic execution of the simulation cases.

> Threat simulation relies on appropriate threat modelling for a comprehensive specification of the threats.

Threat modelling is a structured activity for identifying and evaluating application threats and vulnerabilities [6]. Perspectives may be adversarial or defensive. From the defensive perspective, the goals are to identify probable vulnerabilities, remove as many of the vulnerabilities as possible and employ countermeasures to reduce the attack risks. From the perspective of adversaries, the targets are to identify holes and vulnerabilities and exploit them to gain access to the objective.

Attack trees (Schneier **Fehler! Verweisquelle konnte nicht gefunden werden.**) aim at modelling security threats by focusing on the different ways attackers may try to attack systems. Based on this knowledge, system developers are more likely to design countermeasures that are able to hinder these attacks.

In attack trees, attacks against a system are represented in a tree structure where the root node represents the attack goal. Branches in the tree represent the different paths an attacker can follow to achieve his or her goal. OR-nodes represent alternatives, while AND-nodes represent subgoals, where all of these must be fulfilled in order for the attack to be successful. The trees can be shown graphically or be written in outline form.
Previous methods show the use of attack graphs to demonstrate the path of a single attacker [8]. But in such models creating an attacker profile is necessary which will not be feasible for unknown attackers. However, attack tree models excel at estimating the risk for situations where events happen infrequently or have never happened before.
While Attack tree technique shows how the system is threatened and exploited by attackers, **Misuse case** technique is "Inverse Use Case" [9] which aids in the analysis of the threats a vulnerability is exposed to, and identification of countermeasures to mitigate the exposure risk.

The attacker is represented as a misuser that initiates the misuse cases, either intentionally or inadvertently. Røstad **Fehler! Verweisquelle konnte nicht gefunden werden.** has extended the misuse case notation to also include the ability to represent insiders and vulnerable system functions as model elements.

The TACIT Threat Database

The TACIT Threat Simulator relies on a collection of cyber threats previously defined in the TACIT Threat Database. The Database is a novel product that includes threats not only over the IT systems but also over the OT systems and devices in the Smart Grid.

The threat modelling in TACIT adopted Attack tree technique mainly because they are simple, reusable, and relatively easy to understand which easies the communication to a non-security expert audience which is usually the case of critical infrastructure designers or operators

TACIT adopted the OWASP risk rating methodology [11] defining for each threat in the database the estimated likelihood and impact factors. The likelihood factors were defined for both vulnerabilities and threat agents, while impact factors included factors related to both business and technical impact
.
Once threat likelihood and impact are estimated, they can be combined to get a final severity rating for a risk. On top of TACIT threat models, it is possible to perform threat analysis based on indicators for cost, technical proficiency of attackers, breach of trust and noticeability.

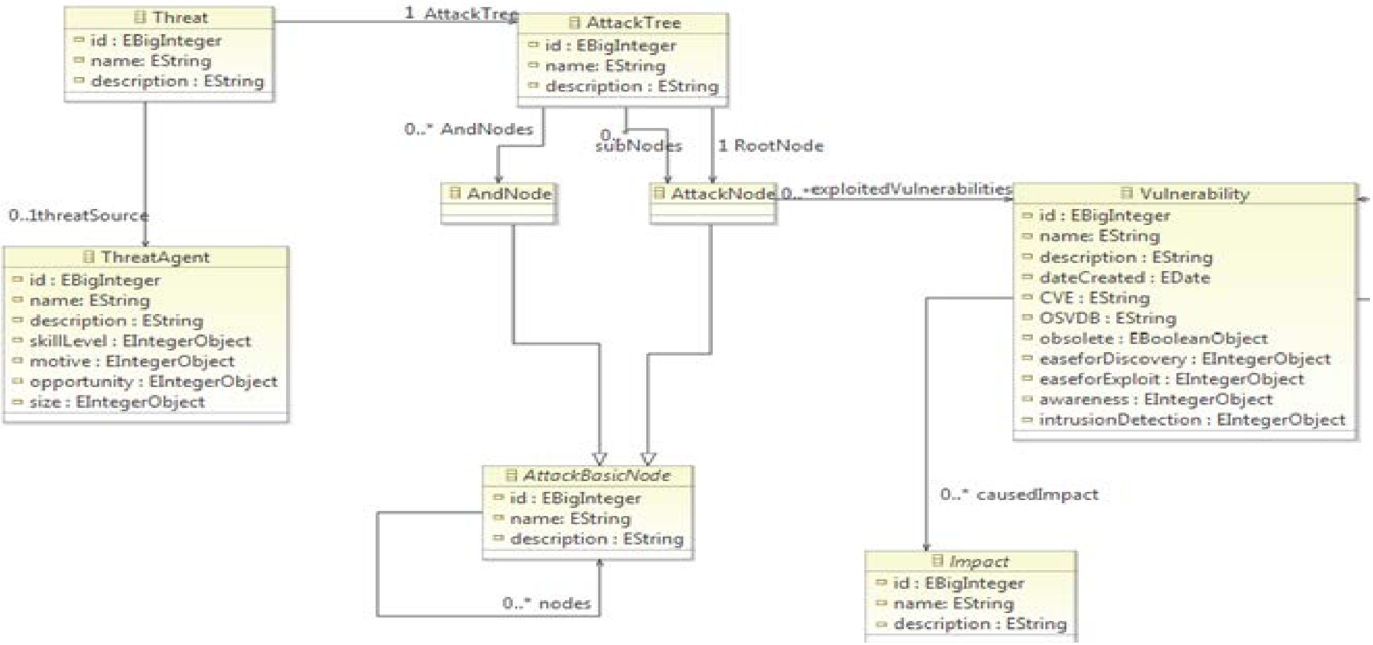


Figure 6: Excerpt of the TACIT Threat model.

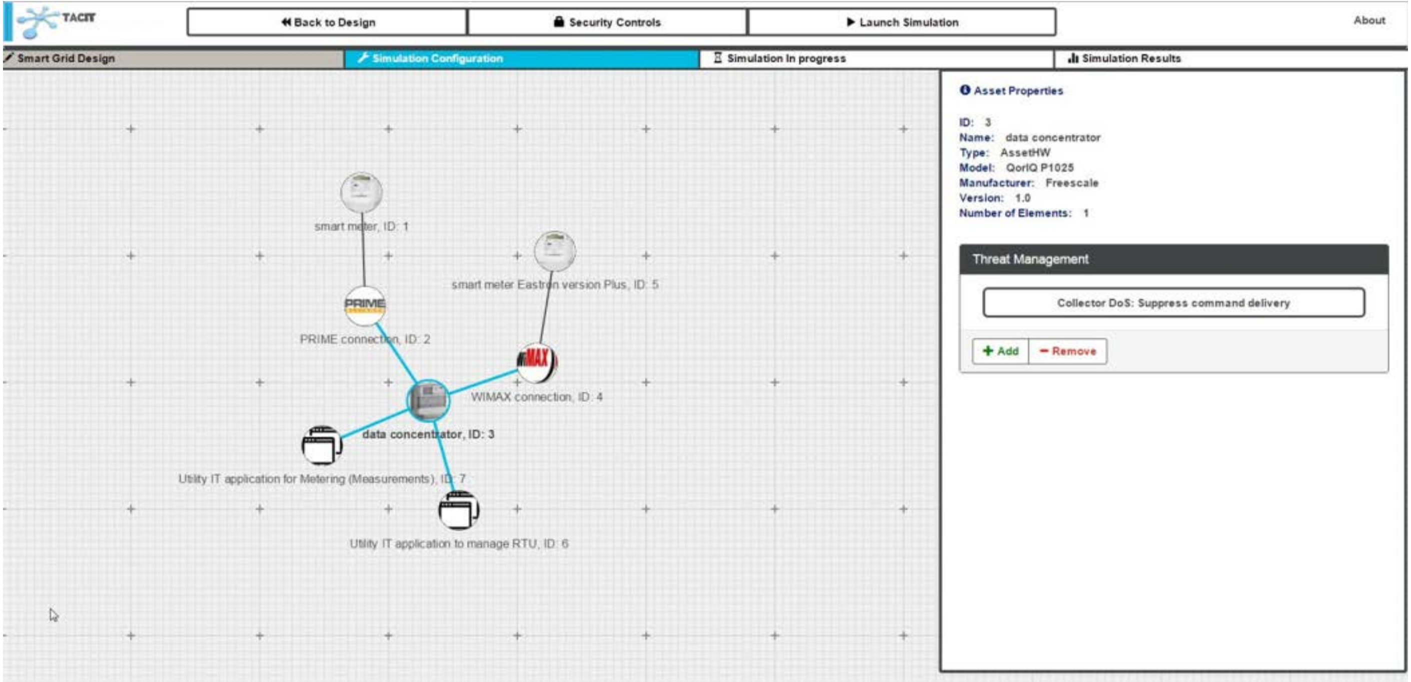
It is worth to note that for the TCP/IP related threats information enrichment, the TACIT Threat Database may be connected to *Vulnerability databases* such as Common Vulnerabilities and Exposures (CVE®) [12], that lists publicly known information security vulnerabilities and exposures, and Open Source Vulnerability Database (OSVDB) web-based vulnerability database [13].

For a more understandable visualisation of the threat impact, the Threat Database can also be connected to *Smart Grid layout databases,* usually owned by Smart Grid developers or Smart Grid owners, which include custom layouts defining the map of existing elements or assets in the Smart Grids.

The TACIT Threat Simulator

The TACIT Simulator enables three main tasks:

- Design the Smart Grid: define the Smart Grid elements and their architecture, including connections and protocols.
- Configure the simulation: define the desired (combinations of) attack(s) to be simulated over the Smart Grid.
- Check simulation results: besides graphically showing attack impact on the smart Grid elements in the layout, the simulator generates simulation logs and reports about:
    - o *Simulation Test Case*: Information about Smart Grid assets and configuration, Attack tree branches simulated and attack nodes in the branches.
    - o *Simulation details*: Information about the attack branches' simulation result, detailing for each attack node the exploited vulnerabilities.
    - o *Impact*: Technical and Business impacts for each exploited vulnerability.
    - o *Recommendations*: For each compromised asset, proposed security controls that could stop the attack.



Asset Properties

ID: 3
Name: data concentrator
Type: AssetHW
Model: QorIQ P1025
Manufacturer: Freescale
Version: 1.0
Number of Elements: 1

Collector DoS: Suppress command delivery

Figure 7: TACIT Simulator - Configuration of attack.

The way forward: Security 360º

Following the path of critical infrastructure protection solutions initiated by TACIT, Tecnalia started in 2015 an innovative endeavour named **Security 360º** for the comprehensive cybersecurity control in Critical Infrastructures such as Smart Grids.

> “Security 360º is a non-intrusive system for **detecting cyber security anomalies and operations** for the Smart Grid through the integral monitoring of communications.”

Security 360º analyses traffic communications in the internal network of a substation and the content of exchanged messages, identifying deviations from the usual operation pattern of the facility.

The analysis is performed in real time and in a non-intrusive way, a particularly relevant feature in a sector with very high response requirements.

Security 360º has been specially conceived for the protection of the Smart Grid, so it covers sector specific standards and protocols.

The system includes machine learning capabilities which enable the detection of new attack patterns based on historical data. Since all data associated with communications is registered it allows forensic analysis of any incident.

References

[1] *The Digital Energy System 4.0. Available from: http://www.smartgrids.eu/documents/ETP%20SG%20Digital%20Energy%20System%204.0%202016.pdf [Accessed 08/02/17].*

[2] *Smart Grid Threat Landscape and Good Practice Guide, ENISA, 2013. Available from: https://www.enisa.europa.eu/publications/smart-grid-threat-landscape-and-good-practice-guide/at_download/fullReport [Accessed 08/02/17].*

[3] *Communication network dependencies for ICS/SCADA Systems, ENISA, 2016. Available from: https://www.enisa.europa.eu/publications/ics-scada-dependencies/at_download/fullReport [Accessed 08/02/17].*

[4] *Threat Assessment framework for Critical Infrastructures protection, TACIT EU-funded project. Available from: www.tacit-project.eu [Accessed 08/02/17].*

[5] *The Cyber Security Report May 2016 by Control Engineering. Available from: http://www.controleng.com/fileadmin/content_files/ce/Control_Engineering_2016_Cyber_Security_Report.pdf [Accessed 08/02/17].*

[6] *T. Olzak, A Practical Approach to Managing Information System Risk, 2008.*

[7] *B. Schneier, Attack Trees. Dr. Dobb's Journal, vol. 24, pp. 21 - 29, 1999.*

[8] *J. Wing, Scenario Graphs Applied to Network Security, Y. Qian, J. Joshi, D. Tipper, and P. Krishnamurthy, Eds. Morgan Kaufmann Publishers, Elsevier, Inc., 2008.*

[9] *G. Sindre and A. L. Opdahl, "Eliciting security requirements with misuse cases," Requirements Engineering, vol. 10, pp. 34-44, Jan 2005.*

[10] *Hilpinen Risto, "Deontic Logic," in Goble, Lou, ed., the Blackwell Guide to Philosophical Logic. Blackwell, 2001*

[11] *The OWASP Risk Rating Methodology. Available from: https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology [Accessed 08/02/17].*

[12] *Common and Vulnerabilities and Exposures (CVE®). Available from: https://cve.mitre.org [Accessed 08/02/17].*

[13] *Open Source Vulnerability DataBase (OSVDB). Available from: http://osvdb.org [Accessed 08/02/17].*

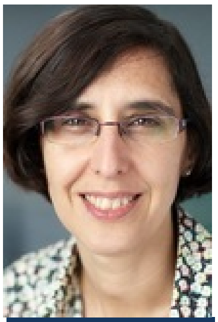
[14] *MUSA www.musa-project.eu*

[15] *EuroCloudCluster https://eucloudclusters.wordpress.com/data-protection-security-and-privacy-in-the-cloud*

Authors’ Contributions

Eider Iturbe

Eider Iturbe is a research engineer of Cybersecurity and Safety team within Tecnalia. She is experienced in trust and security engineering technologies and is currently leading the architecture and integration work package in EU H2020 MUSA project, on multi-cloud secure applications. Eider graduated in Telecommunication Engineering from the University of the Basque Country (Spain) and in the European Master in project management at the same university.



Mª Carmen Palacios

Mª Carmen Palacios is a research engineer of Cybersecurity and Safety team within Tecnalia. Her knowledge and research interests focus on security and safety concepts applied to critical systems. She is currently involved in H2020 COSSIM and MUSA European projects. She is graduated in Physics (Electronics & Automation) from the University of the Basque Country (Spain).

Spatial-aware Iterative Integration of Crisis Management Information Systems

The goal of the FP7 project PREDICT is to provide a comprehensive solution for dealing with cascading effects in multi-sectoral crisis situations covering aspects of critical infrastructures. The result leverages on integrating specialised innovative information systems.

Information systems are playing an increasingly more important role in modern crisis management process. An integrated system with capabilities like foresight, prediction and decision support can provide substantial added-value for decision makers on both tactical and policy-making levels. It is however a challenging task to seamlessly integrate various systems with dedicated functionalities on functional and technical aspects, especially when these systems are developed independently from each other with substantially different design rationale and software technology. In this article, an iterative system integration approach is proposed by harmonising service-oriented, model-driven and agile system development. Several design principles and best practices from the software engineering community are adopted to facilitate the integration task. In addition, extra attention is paid to provide enhanced support for integrating spatial data into the crisis management workflow. This approach aims to provide a pragmatic system integration methodology to integrate crisis management information systems in a more effective and efficient fashion.

Iterative system integration

Working with partners from different organisations on the same software project can be difficult, especially when it comes to integrating new system features and providing system maintenance. It can yield unwanted dependencies and slow down the software development process. Therefore, a modular software architecture can help to manage system development and decouple component dependencies. In the following subsection, four major aspects of the integration approach are elaborated.

RESTful service-oriented architecture

Service-Oriented Architecture (SOA) is an architectural design pattern based on isolated and de-coupled software components—each provides dedicated services to the others, focusing on interoperability and re-usability. One approach to implement SOA capability is using RESTful web services, which provide lightweight and highly scalable solutions. Extensive programming language support and a large ecosystem make it ideal for integrating heterogeneous information systems used in the crisis management process. Figure 8 illustrates a system with three services and a proxy. All three services can be developed independently by different organisations. They are accessible by exposing themselves via the proxy, which decouples the service interface and the implementation. This kind of system isolation is crucial for developing different crisis management system components.

Iterative Integration

An iterative approach of system integration can be separated into three stages:

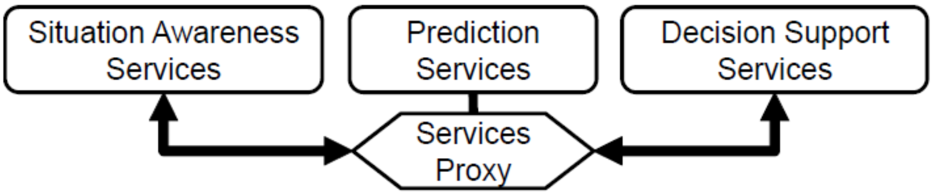


Figure 8: A service suite with three RESTful web services and one service proxy. Each of them provides dedicated services and can communicate with each other via the proxy

Jingquan Xie

Fraunhofer IAIS, Germany and has been working in projects focusing on Critical Infrastructure Protection (CIP): IRRISS, DIESIS, EMILI, VASA, CIPRNet and PREDICT. His main research interests are database management systems, knowledge engineering.

jingquan.xie@iais.fraunhofer.de

Betim Sojeva

Betim Sojeva is a research associate at Fraunhofer IAIS. He has experience in Computer Vision and Computer Graphics as well as in Web technologies and Geographical Information Systems (GIS).

betim.sojeva@iais.fraunhofer.de

1) Defining specification and requirement of the service. This includes developing use cases, formal specification, etc.
2) Writing service mock-ups and deploy them to the server for automated testing. After this stage, all unit tests should pass as required in classical Test-Driven Development (TDD).
3) Iteratively replacing mock-ups by real implementations. Each time, if a service mock-up is replaced, all unit tests must be executed to guarantee that the service implementation meets the requirements defined in the specification.

Embracing Software Containers

Component-based development is a technique to manage software artefacts on a single or on multiple host machines. A software container is an isolated and independent auxiliary software piece that hosts other software components. Once deployed, a software container can be considered as a running application with all the dependencies it needs. In the iterative approach used in PREDICT, several software components used for the deployed integrated system and during its development are "packed" into containers, including: the Web Server for the web based user interface, Documentation Server, Map Services, Data Storage, and Continuous Integration server.

Spatial Data Integration

Spatial data integration is an essential part in the modern crisis management process. Most of the objects that are of interest to the crisis management team have geographical locations—like a street, a telecommunication router, an electrical substation, etc. Crisis managers and situation operators need sufficient information about the states of these objects, in order to make reasonable decisions like whether to evacuate a certain region.

Modern geographical information systems consist of a set of standards like Web Map Service (WMS) and Web Feature Service (WFS) to facilitate the modelling of these objects. A dedicated map server can be set up as a container providing spatial data support. The descriptions of objects that need to be rendered by the map server can be extracted from another container that implements Data Storage.

Use case—the integrated PREDICT tool suite

The integrated PREDICT tool suite—iPDT for short—developed in the PREDICT project is an example that realises the proposed integration approach. The fully integrated system iPDT combines the component systems on both conceptual and technical level. Each of the blocks in Figure 9 corresponds to a Docker container—a proprietary implementation of software containers.

Services provided by component systems like PROCeed or MYRIAD are specified at the beginning and replaced iteratively by implementations provided by different organisations. This kind of isolation and decoupling make the distributed development and deployment more efficient. Moreover, information generated within iPDT can also be fed into other systems. For instance, the information forecast by PROCeed can also be fed into other systems by providing the standard mapping services on top of the Web. Currently a working group in the PREDICT project is focusing on integrating the Dutch national crisis management system LCMS with iPDT by applying this kind of spatial-aware integration approach. Finally, all the services are deployed by using the high performance reverse proxy server NGINX.

Based on current situation information, iPDT computes likelihoods of fictitious future scenarios and determines a set of most likely scenarios (SBR, scenario based reasoning). For these scenarios, iPDT provides information related to cascading CI effects (PROCeed tool). The combined results are fed into MYRIAD, which evaluates the situation information according to certain metrics in order to further eliminate less likely possible scenarios. For example, the fictitious future scenarios could describe CI outages of different lengths and indicate consequences of the outages and limitations of response and mitigation actions dependent on the duration of the outage.

The PREDICT Consortium

- Research & Technology Organisations: CEA, Fraunhofer, VTT, and TNO.
- End-user organisations: the International Union of Railways (UIC), the Safety authority of South-Holland-South Region, and the Finnish environment institute (SYKE).
- Large industry actors and SMEs with a strong expertise in crisis management: CEIS, Thales, and iTTi.

Find out more about PREDICT at www.predict-project.eu

Disclaimer: The project PREDICT has received funding from the European Union's Seventh Framework Programme (FP7/2007-2013) under grant agreement n° FP7-SEC-2013-607697. The contents of this article do not reflect the official opinion of the European Union. Responsibility for the information and views expressed herein lies entirely with the authors.

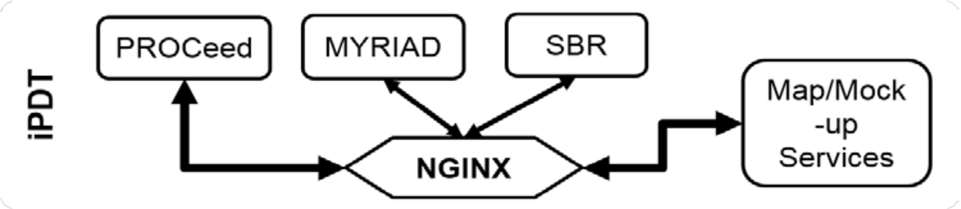


Figure 9: The integrated PREDICT tool suite consisting of three major components – PROCeed, MYRIAD and SBR including mapping service and the service mock-ups.

EU-CIRCLE: A pan-European framework for strengthening Critical Infrastructure resilience to climate change

The aim of the Horizon 2020 project EU-CIRCLE is to develop a framework and a set of tools that will enhance the resilience of interconnected Critical Infrastructure Networks to climate hazards under climate change.

Climate related hazards (e.g. floods, storms, extreme precipitation, wildfires etc.) have the potential to destroy or substantially affect the lifespan and effective operation of European Critical Infrastructures (CI), such as energy, transportation, ICT and water infrastructures. When infrastructure systems are damaged or fail, the smooth functioning of society is disrupted. To further complicate matters, modern infrastructures operate as a 'system of systems' with many interactions and interdependencies among these systems. Damage in one infrastructure system (e.g. ICT) can cascade and result in failures and cascading effects onto all related and dependent infrastructures (e.g. energy and water infrastructures).

Critical Infrastructures are designed and constructed in accordance with national building codes and infrastructure engineering standards (e.g. EUROCODES). These set out climatic design values that aim to build resilience to climate hazards, for example return periods for extreme weather events. Most existing infrastructures have been designed with the assumption of stationary climate conditions using historic values and observations. Stationarity assumes that although climate is variable, these variations are however constant with time, and occur around an unchanging mean state. This assumption of stationarity is still common practice for design criteria for (the safety / security levels of) new infrastructure.

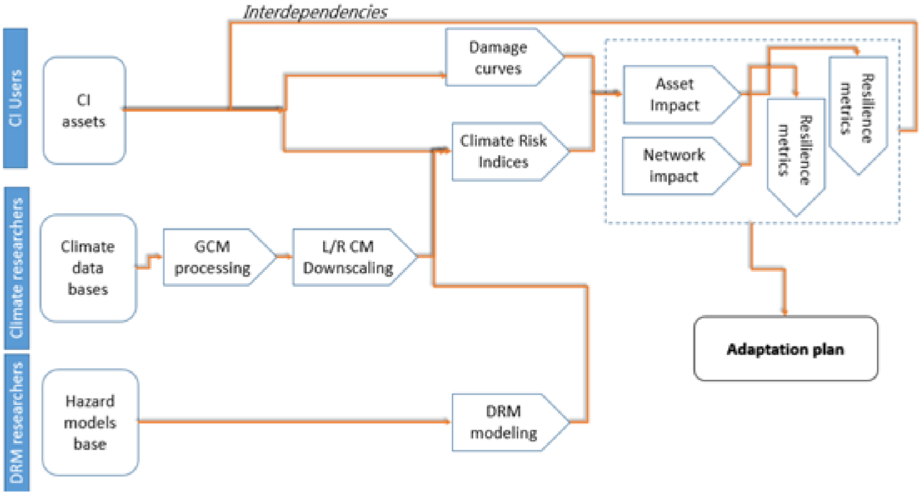
However, the climate is changing: the atmosphere and oceans have warmed, global temperatures have risen by 0.85 ° C, and sea levels have risen by 19cm since pre-industrial times. There is evidence that the increase in global temperatures has resulted in an increase in the ***intensity*** and ***frequency*** of extreme weather events. As return periods of extreme weather events are calculated using past historical climatic data, under climate change weather extremes will tend to exceed the design specifications for CI more frequently and earlier during the lifetime of an infrastructure, decreasing the durability and resilience of the structure. The changing climate will, in effect, shorten the lifespan of existing CIs in many regions.

The main strategic objective of EU-CIRCLE is to move towards an infrastructure network(s) that is resilient to today's natural hazards and prepared for the future changing climate. It aims to contribute to the EU's Adaptation Strategy through the promotion of better decision-making by addressing existing gaps in the knowledge on climate change impacts and adaptation in CIs. EU-CIRCLE aims to achieve this by defining a proper conceptual framework and development of tools for enhancing the resilience of critical infrastructures to climate stressors.

Athanasios Sfetsos

Dr. Athanasios Sfetsos is a Researcher at the National Center for Scientific Research "Demokritos". He is the coordinator of EU-CIRCLE project: A pan-European framework for strengthening Critical Infrastructure resilience to climate change. His research interests are related to the impacts of climate change and critical infrastructure protection.

e-mail: ts@ipta.demokritos.gr



EU-CIRCLE Resilience Framework

The EU-CIRCLE climate resilience management framework is based on: a) the identification of the critical assets/processes of an infrastructure network that provide essential services to society; b) the determination of the critical values and/or patterns of climate parameters that result in a change of state for these assets (in terms of performance or functionality); c) the analysis of the relative impact, determined using appropriate consequence or damage curves; d) consequence analysis to determine cascading effects arising from interdependencies (including physical, cyber, geographic, and logical) and their related impacts; and e) analysis of the coping and adaptive capacities of the asset/network/society (resilience) which in turn leads to the identification of adaptation plans/programmes/strategies and investment needs.

EU-CIRCLE Risk Assessment Framework

The first step to improving resilience of CI to climate change impacts is the identification of the risks of several climate hazards to interconnected and interdependent critical infrastructures i.e. risk assessment.

The EU-CIRCLE risk assessment framework includes:

- Assessment of the current risks of a specific climate hazard to a single CI or a CI network or even an area of interest with interconnected and interdependent CI.
- Examination of how climate change may alter risk in the future, or expose new risks. This analysis includes a baseline assessment of the risks to CI assuming no additional adaptation actions under various climate change scenarios, as well as a second assessment which considers how current or future potential adaptation actions will affect the overall scale of risk to CIs in the future under the same climate change scenarios.
- Identification of climate change adaptation or risk mitigation options and definition of priorities. This step examines alternative strategies for mitigating risks to CI and strengthening their resilience such as: enhancing the defences of interconnected infrastructures and implementation of long term adaptation options.

A comparative assessment of these scenarios using well identified criteria (e.g. cost – benefit analysis) will return scientific evidence for supporting informed decision making.

EU-CIRCLE Climate Resilience Platform

CI vulnerabilities to climate hazards and impacts from extreme weather events go beyond physical damages. EU-CIRCLE will provide an assessment framework that also takes into account the impacts to the services provided by CIs, the impacts associated with repair and/or replacement of services but also, societal costs, environmental effects, and economic costs due to suspended activities.

Such assessments will be carried out on a validated Climate Infrastructure Resilience Platform (CIRP). The CIRP is a standalone and comprehensive software toolbox that is able to accommodate different types of datasets (e.g. hazard, assets, interconnections, fragilities), file formats, and risk analysis algorithms. It is open, modular and extensible in order to support various risk and resilience assessment analysis tools.

> CIRP provides a platform for assessing the impacts of climate change and extreme events on interconnected critical infrastructures.

CIRP will provide users with access to diverse simulation, modelling and risk assessment solutions. This modelling approach will support planners, operators and authorities to assess the impact of alternate climate change scenarios on the operation and performance of CIs, including any potential cascading effects due to interdependencies between CIs. It is intended to be a user-friendly environment that will provide its users with the ability to analyse what-if scenarios: leveraging model selection, climate data repositories, and CI inventories in order to calculate damages for any kind of climate hazard and CI.

EU-CIRCLE Exercise

On 7 and 8 of March 2017, the EU-CIRCLE consortium will be conducting an exercise in Cyprus aimed at Critical Infrastructure Operators. The exercise is co-organised with the Cyprus Civil Defence (National Contact Point for EPCIP). The exercise will explore the effects of two scenarios: flash flooding and forest fires on critical infrastructure in Cyprus under conditions of climate change. The scenarios will model projected climate change for Cyprus based on the Representative Concentration Pathways (RCPs) of the Intergovernmental Panel on Climate Change (IPCC) and in particular RCP 2.6, RCP 4.5 and RCP 8.5 for the time period 2016 to 2050. The exercise will showcase the CIRP and show how the risk assessment and resilience frameworks developed by EU-CIRCLE can be used with CIRP to model the potential impacts of climate hazards in a changing climate and allow for adaptation plans to be developed.

The EU-CIRCLE Consortium

The EU-CIRCLE Consortium consists of 20 partners: National Center for Scientific Research –Demokritos (GR); Fraunhofer-Gesellschaft Zur Foerderung Der Angewandten Forschung E.V (DE); Meteorologisk Institutt (NO); University of Exeter (UK);Gdynia Maritime University (PO); ARTELIA Eau et Environnement SAS (FR); SATWAYS Ltd (GR); Entente pour la forêt Méditerranéenne | Valabre (FR); D'Appolonia S.P.A. (IT); Državni Hidrometeorološki Zavod – Meteorological And Hydrological Service (HR); XUVASI Ltd (UK); MRK Management Consultants GmbH (DE); European University of Cyprus / Center for Risk and Safety in the Environment (CY); Center for Security Studies (KEMEA) (GR); University of Salford (UK); National Protection and Rescue Directorate of the Republic of Croatia (HR); ADITESS Ltd (CY); Torbay Council (UK); HMOD-Hellenic National Meteorological Service (GR); University of Applied Sciences Velika Gorica (HR).

If you would like to find out more about EU-CIRCLE please visit our website at http://www.eu-circle.eu

A Good Practice Guide on Critical Information Infrastructure Protection

A Guide for Governmental Policy-makers.

Early 2016, the Meridian Process and the GFCE tasked the Netherlands Organisation for Applied Scientific Research TNO to develop a Good Practice Guide on Critical Information Infrastructure Protection (CIIP) for governmental policy-makers [1]. The guide primarily aims at governmental policy-makers, but other stakeholders such as Critical Infrastructure (CI) operators may benefit from the guide as well. The guide starts at the bottom end where no experience exists with CI protection and CIIP, but also provides insights and angles of incidence which can be of help to those who already have taken steps towards a more mature CIIP posture.

Guide to assist nations in their CIP – CIIP journey

The Meridian Process [2] aims to exchange ideas and initiate actions for the cooperation of governmental bodies on CIIP. The Global Forum on Cyber Expertise (GFCE) [3] is a global platform for nations, international organisations and private companies to exchange and generate best practices and expertise on cyber capacity building. GFCE's aim is to identify successful policies, practices and ideas and multiply these on a global level by developing practical initiatives to build cyber capacity worldwide.

Structure of the GP Guide

The guide starts with an introduction explaining the need for CIIP, the distinction between CII, CIIP and cybersecurity, and how to use the guide. Six topic-oriented chapters follow, each with a general description, an explanation of the main challenges, good practices and references for further reading. The six key topics (see figure 3) are:

- National perspective
- Identification of national CI
- Identification of CII
- Developing CIIP
- Monitoring and continuous improvement
- Networking and Information Sharing

Understanding CII

The guide starts explaining that one needs to understand one's CI first. Although nations have defined the notion of CII (see: CIPedia© [4]), the identification of CII is difficult as it comprises two dimensions: the critical information and communication "backbone" (e.g. telecom, internet), and critical functions in CI such as the process control/SCADA environment in the energy sector, financial transaction systems, and alike.

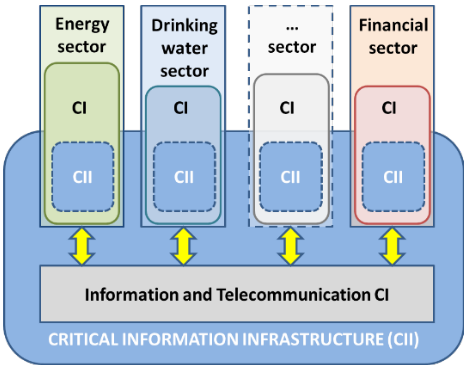


Figure 1: Critical Information Infrastructure

From Figure 1, it will be clear that CIIP efforts in many nations cross the boundaries of public and private organisations, and of CI sectors. CIIP also touches upon issues like trusted supply chains and trusted sourcing of hardware and software.

Highlights

The guide outlines five sequential steps to address the complex CIIP challenges (see Figure 3): the first five key steps mentioned in the list above. The sixth is both a topic and a step: 'networking and information sharing' is essential on its own and supports each of the first five key steps.

Under the national perspective topic, a national risk profile approach is proposed to balance the various threats with the need for protection of CI and CII. For example, in case the power grid is hampered by daily disruptions in its supply of energy, national priorities may less worry about CIIP. Moreover, CIIP requires a multi-stakeholder / multi-agency co-operation within administrations.

Eric Luiijf
is principal consultant at the Netherlands Organisation for Applied Scientific Research TNO. He contributed both at the technical and policy levels to many national and EU Critical (Information) Infrastructure Protection projects since 2000,

e-mail: **eric.luiijf@tno.nl**

Tom van Schie

joined TNO as a junior consultant cyber security. He obtained his master degree in the United Kingdom and Germany on International Security. He has a keen eye for cybersecurity policy and governance issues, but also for technical developments. He has worked for the Dutch National Cyber Security Centre (NCSC) advising on international affairs, public-private partnerships and cybersecurity trends.

e-mail: **tom.vanschie@tno.nl**

Sometimes not easy but crucial for a balanced and effective approach.

Based on the national risk profile, one can identify the CI, CI sectors and critical services. A dependency analysis should follow, which takes cross-border aspects into account as well. It is beyond dispute that this requires interaction with all stakeholders: agencies and CI operators. The identification of the National CI (for definitions: see CIPedia [4]) is a required step before one should consider CIIP.

The identification of the CII is the next complex step. As discussed above, it requires the cooperation of multiple agencies and may also involve other organisations like CI operators. Note that the guide does neither presume, nor exclude a priori any specific government, legal, governance, or other structure. It merely mentions the issues and challenges to be addressed in one's own national context, way of working, etcetera.

One threat to be addressed comprises CII dependencies. The tricky aspect with dependencies is that they sometimes stem from unexpected sources. Or better said, overlooked critical services such as the national domain name registry, a certificate supplier, a crucial glass fibre, or a cloud services provider. New technologies may alter the set of CI/CII dependencies and thereby the risk landscape in a rapid way. The guide touches all these issues.
Note that some of these dependencies may not be recognised yet by nations which have a more mature posture in CIIP.
For that reason, the last section of the sequence

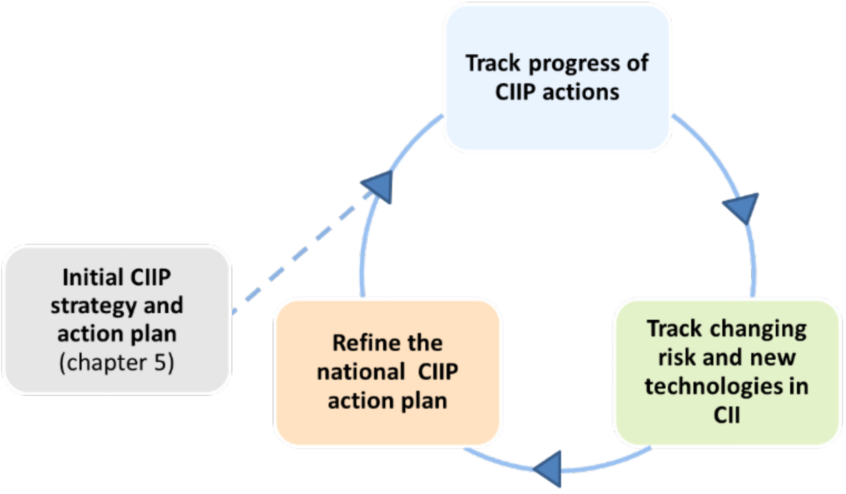

Track progress of CIIP actions
Track changing risk and new technologies in CII
Refine the national CIIP action plan
Initial CIIP strategy and action plan (chapter 5)

Figure 2: Continuous CIIP improvement cycle

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.

… and more

The guide was presented at the Meridian conference in Mexico City and can be downloaded for free since then. Translation from English into other languages is encouraged (see the colophon section of the guide). Actually, a Spanish translation effort has come to the attention of the authors.

References

[1] Eric Luiijf, Tom van Schie, Theo van Ruijven, Auke Huistra (2016), Good Practice Guide on Critical Information Infrastructure Protection (CIIP) for governmental policy-makers: https://www.tno.nl/gpciip/
[2] Meridian: www.meridianprocess.org
[3] GFCE: www.thegfce.com
[4] CIPedia©: www.cipedia.eu

email eric.luiijf@tno.nl

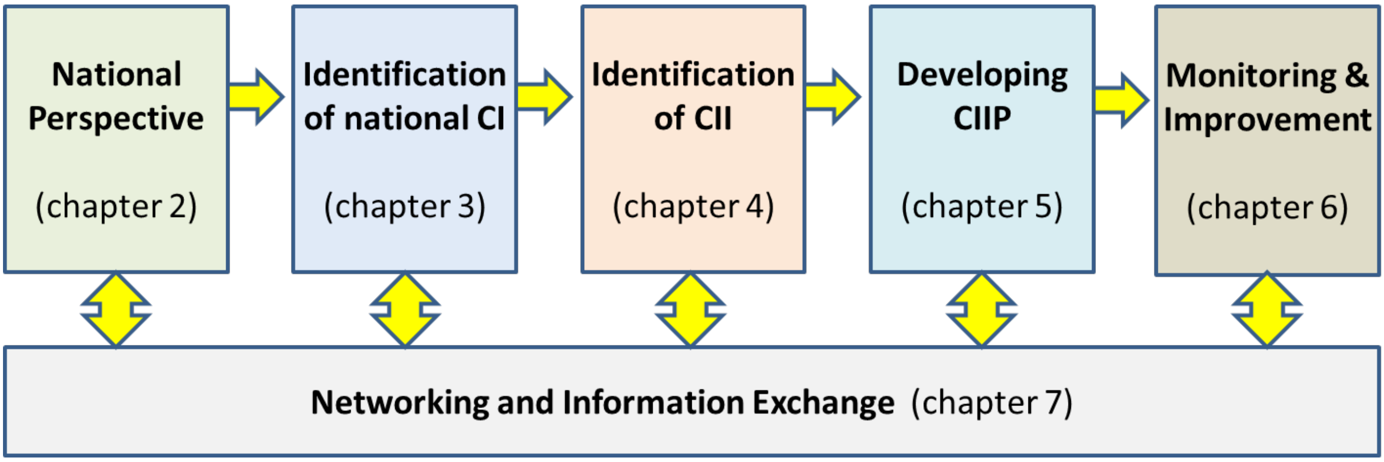

National Perspective (chapter 2)
Identification of national CI (chapter 3)
Identification of CII (chapter 4)
Developing CIIP (chapter 5)
Monitoring & Improvement (chapter 6)
Networking and Information Exchange (chapter 7)

Figure 3: Outline of the guide's topics

Human vulnerability mapping facing critical service disruptions for crisis management

The goals of these researches are to improve the automated assessment of consequences facing simulated scenarios of critical service disruption. They are situated at the crossing between the FP7 project CIPRNet and the French project DEMOCRITE.

Civil safety institutions are well prepared to strong crisis, but it is known that the cascading effect management is a hard point of the preparation. It necessitates the understanding of each Critical Infrastructure (CI) functioning, but also the knowledge of the global system behaviour facing a crisis. For helping crisis managers to have a better awareness on cascading effects, some tools propose to model CI dependencies. However, the crisis management requires on top of these cascading effect simulations a timely, accurate and realistic assessment of the consequences of a scenario, especially on the population. This common concern has been identified by at least two research projects: CIPRNet and DEMOCRITE. Both are presented below and their new approaches of the consequences assessment are complementary.

The CIPRNet tools model cascading effects between CI and assess human impacts in an innovative but static manner: people are located at their census home; their sensibility to a resource lack varies during the day. The methodology developed for the DEMOCRITE project improves it by mapping people mobility. It focuses on location of people with regards to their activities and the time period (night/day, holidays), and discuss their sensibility to the lack of key infrastructure services.

The CIPRNet project and its method for assessing consequences

The Critical Infrastructure Preparedness and Resilience Research Network or CIPRNet is a European FP7 project that establishes a research network on CI Preparedness and Resilience. This project runs until February 2017 and is under the coordination of the Fraunhofer. The CIPRNet Decision Support System (DSS) already developed comprises five parts:

1. an operational DSS, gathering of real time external inputs like the weather forecast;
2. an event simulator, modelling of natural events for scenarios;
3. a harm simulator, estimating infrastructures damages;
4. an impact assessment tool, modelling cascading effect between CI;
5. a What-if analysis tool, comparing strategies of emergency response based on the consequences estimation.

We are interested here in this last part. Four criteria evaluate the consequences: the human impacts, the access reduction to primary services on the territory (access to wealth structures, schools, and so on), the economic losses and the environmental damages. They are caused either directly by the event, or indirectly by cascading effects. This point is measured by a service disruption in terms of electricity, telecommunications, water (drinking water, waste water), gas and other energetic products and mobility (availability of roads and railways transport).

Amélie Grangeat

PhD. student Amélie Grangeat is an engineer in risk management working in the CEA (Fr). She is currently involved in four research projects around the critical infrastructures protection: DEMOCRITE (Fr), CIPRNet (FP7), RESIWATER (Fr-Ge), and PREDICT (FP7). The two first projects are described here, the others concern the resilience of the water utilities for RESIWATER, and the crisis management for PREDICT. Her research has been awarded by the CIPRNet Young Critis Award 2016.

e-mail: **amelie.grangeat@cea.fr**
amelie.grangeat@orange.fr
CEA/Gramat
46500 GRAMAT
FRANCE

The human impact assessment method developed in CIPRNet uses an innovative perspective. Having no water is a problem only when you need it, and this remark may be applied to others critical services. For this reason, the CIPRNet consequences assessment is based on Service Availability Wealth (SAW) Indexes, determining the relevance of the service availability as a function of time and of the population's vulnerability. This last one is split into four categories: old, young, disabled people and others.
The CIPRNet team gathers statistical data on the consumption of primary technological and energy services like average monthly household expenditure on electricity or gas, to compute the relevance indexes of each service.

At the end, a typical day (working vs. non-working day) with time schedule and statistical activities is proposed. For instance, electricity use during a day is split into nine different functions: lighting, refrigerator/freezer, air conditioning, TV, oven, microwave, washing machine & dryer, and a global section for other appliances. Evaluating the importance of various activities requiring services within a daily time schedule, CIPRNet project obtains a normalised indicator of relevance of services (SAW Indexes) for each service and each category of citizen every 30 minutes.

The CIPRNet method on consequences assessment crosses the SAW indexes with the availability and the quality of the critical service as a function of time and localisation. It enables by this way to compare the gravity of the different calculated scenarios in an automated manner with an innovative approach.

However, this approach of assessing human impacts by using citizen's activities at home is static. For instance, the relevance of service availability in accommodations drops to zero during the working hours because people are outside. But it does not grow in other buildings because we don't know the people localisation during these working hours. In order to improve it, it seems necessary to complete this assessment by the human density mapping and its daily evolution. This work has been done with the DEMOCRITE project, presented below.

The DEMOCRITE project presentation and its method for mapping the human vulnerability

Having statistical information on people location is a significant help for safety institutions. Accurately estimating the population exposure is important for assessing crisis consequences. This precision means to understand the spatiotemporal variation of the population distribution and not to rely only on census static data. The Ile-de-France French civil safety institution handles a research project named DEMOCRITE to map dynamically (among other tasks) human vulnerability in Paris. We define "human vulnerability" of one territory as the spatiotemporal distribution of people: the more concentrated is the population, the more important is the human vulnerability. They are a "vulnerability" in the sense that people are the main stake to protect during a crisis, facing a threat. The method developed in this project is presented below and on the figure.

A week has been divided into three periods (Weekdays, Saturdays, Sundays) and each day has been divided into four time slots: the morning rush hour, the daytime, the evening and the night.

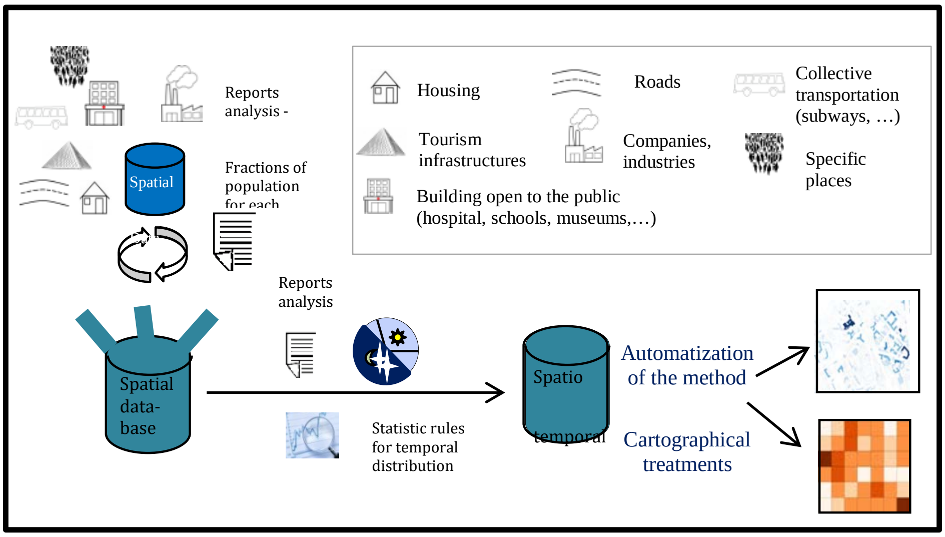
In total, more than 70 spatial databases were used. Only the more complete and accurate were retained. The main challenge was to transform these spatial databases into a spatio-temporal database.

The temporal distribution is calculated according to statistic treatments of available reports concerning the living habits in Paris (opening hours of museums, underground frequentation during a working/non-working day and so on). It enables us to simulate how many people may be in the buildings as a function of the buildings categories and the time slot.

For instance, based on geographical census data and of various statistics on population (age, unemployment, etc.), it is possible to deduce the percentage of people staying at home, including the percentage of unemployed people, young babies and retired people. The same statistical approach is used to estimate people present in shops: based on the shopping surfaces of buildings, one can deduce the maximum capacity of shoppers, and based on statistics on hourly shopping habits, one can calculate the potential numbers of people in these places.

In the same way, education buildings are assumed to be full during class hours but empty during the night, such as the companies' buildings and so on. The visitor numbers of museums and tourist sites are investigated and are associated with their opening hours. Moreover, the number of subway users is also analysed to obtain temporal distribution of people in the subway stations.

Even if this database is not exhaustive and has some imprecisions, it is nevertheless a very useful tool to assess the statistic spatiotemporal distribution of population in Paris.


Reports analysis -
Spatial
Fractions of population for each
Housing
Roads
Collective transportation (subways, …)
Tourism infrastructures
Companies, industries
Specific places
Building open to the public (hospital, schools, museums,…)
Reports analysis
Spatial data-base
Statistic rules for temporal distribution
Spatio temporal
Automatization of the method
Cartographical treatments

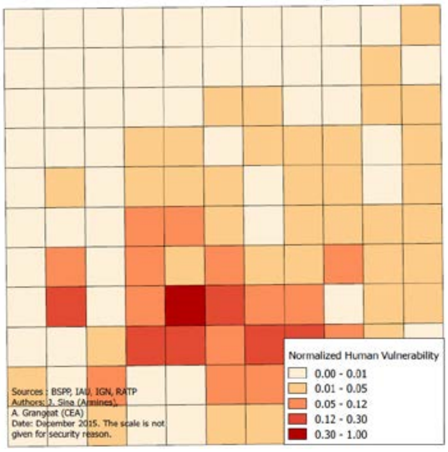
Flowchart of the DEMOCRITE methodology

Finally, the method is automated and proposes maps of vulnerability by counting people present in each mesh composing the territory for the different period of times identified.

Human vulnerability Mapping: some results

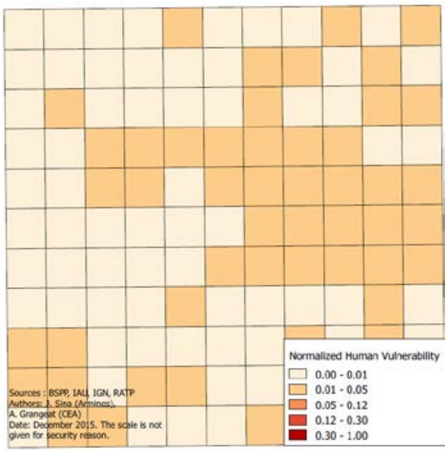
The following maps (illustrative examples) show the evolution of human vulnerability between the night (census data and hostel occupancy rate) and the working hours. The information concerning people's locations and number is gathered and aggregated in a grid mesh (the scale and localisation is not given for security reasons). The represented value in each small mesh is the number of persons present in this small mesh normalised by the highest value obtained over all the periods studied and over the overall mesh.

Human vulnerability maps during a working day



Sources : BSPP, IAU, IGN, RATP
Authors: J. Sina (Armines),
A. Grangeat (CEA)
Date: December 2015. The scale is not given for security reason.

Human vulnerability maps during the night



Sources : BSPP, IAU, IGN, RATP
Authors: J. Sina (Armines),
A. Grangeat (CEA)
Date: December 2015. The scale is not given for security reason.

Conclusion and perspective

The high difference of human density between these two maps shows the importance to take into account the mapping of the human vulnerability when assessing consequences of the scenarios. Maps on the other time slots are discussed in the CRITIS article[1].

This human vulnerability mapping is complementary of the CIPRNet consequences assessment method. Indeed, it enables the possibility to extend the use of relevance index to other places and activities (schools, museums, and so on) and to combine it with the number of people concerned by one critical service disruption. This means improving the accuracy of the consequences assessment.

Once the automated assessment of the scenarios consequences has reached a reliable level and provides accurate information, the next step concerns the huge debate on the definition of quantitative gravity state. How to identify the minimum duration of critical service disruption before being in a crisis, as a function of its localisation? This question has to be studied from a societal and political point of view, and is not closed to have a fix answer.

> Human vulnerability maps of Paris area during periods of a working day time show the importance to take into account people mobility when assessing crisis impacts.

Article and co-author

This work is the result of collaboration and has been published with more details in the following reference.

[1] Grangeat, A.[a] , Sina J.,[b] Rosato V.[c] Bony, A.[b], Theocharidou M.[d] (2016) Human vulnerability mapping facing critical service disruptions for crisis managers. To be published in the Revised Selected Papers on the 11th *International Conference, CRITIS,* Paris, France, October 10-12 2016. 12p.

a. CEA, DAM, GRAMAT, F-46500 Gramat, France
b. Institut des Sciences des Risques – Centre LGEI, Ecole des mines d'Alès, 30100 ALES, France *julie.sina@hotmail.fr aurelia.bony-dandrieux @mines-ales.fr*
c. ENEA Casaccia Research Centre, Roma, Italy vittorio.rosato@enea.it
d. European Commission, Joint Research Centre. Space, Security and Migration. Technology Innovation in Security Unit, Ispra (VA) Italy *marianthi.theocharidou @jrc.ec.europa.eu*

CIPRNet Consortium

All the information on CIPRNet may be found on the CIPRNet project website: http://ciprnet.eu

DEMOCRITE consortium

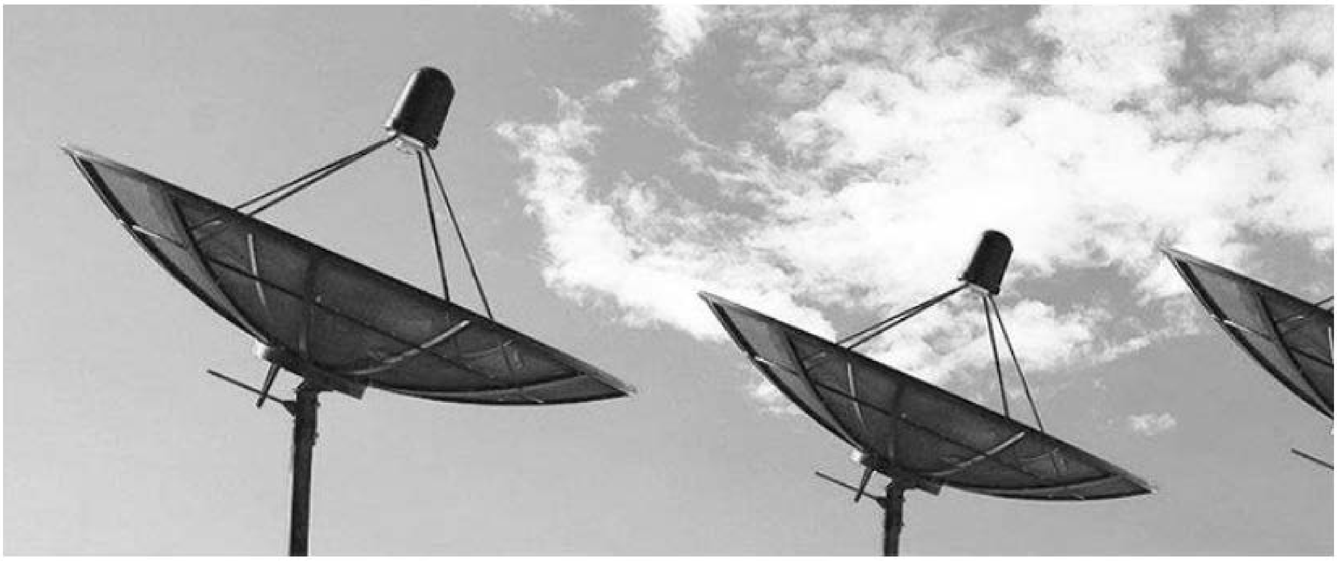
All the information on DEMOCRITE may be found on the DEMOCRITE website: www.anr-democrite.fr

Acknowledgments

The work presented in this paper has been also partially funded by the CIPRNet (Grant agreement no: 312450) European project. The views expressed in this document are purely those of the writer and may not in any circumstances be regarded as stating an official position of the European Commission. The authors want to thank also the French DEMOCRITE (ANR-13-SECU-0007) project for the partially funding of these researches.

euconcip European Cooperation Network on Critical Infrastructure Protection

(/index.php)



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

Protecting Industry 4.0 against Advanced Persistent Threats

As APTs will undoubtedly target Industry 4.0 deployments, it is essential to develop detection mechanisms and architectures tailored to this context

CIIP and the Industry (4.0)

The SADCIP project has arisen from the need to deal with increasingly intelligent and autonomous industrial and monitoring systems, capable of collaborating with each other to meet a common objective: provide efficient and real-time manufacturing and logistics from anywhere, at any time and anyhow [1]. However, any new condition that implies open communication with the Internet and the adaptation of heterogeneous (wireless) systems can, certainly, bring about numerous interoperability and security problems [2].

What types of problems? From a slight fault or anomaly within the operational applications, to massive and distributed attacks of a subtle and potentially damaging nature. Such problems can even have an aggressive effect on the welfare of other critical infrastructures. It is not the same to protect all those operational elements involved in the construction of each component that forms, for example, a bicycle, as the components that comprise a system of transport of greater reach, such as, a plane or a train. Therefore, it is self-evident that there is a relationship between the need to protect today's industry and the need to ensure protection, at all levels, of the rest of the dependent, critical infrastructures. In addition, this characteristic underlines the criticality degree of a new paradigm related to the Internet of Things known as Industry 4.0, which in itself, can also be considered as a critical infrastructure.

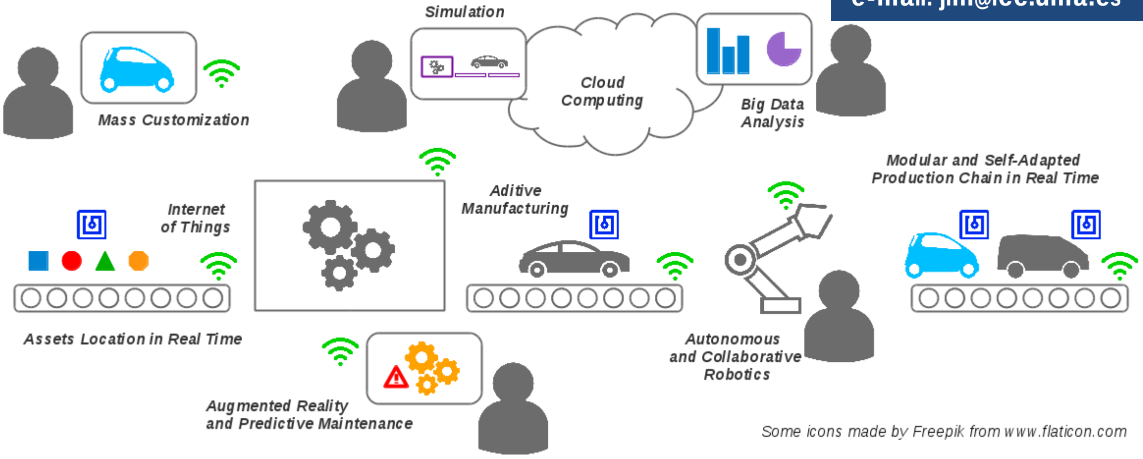
Industry 4.0 (cf. Figure 1) constitutes a technological progress within the traditional industry. Here, both novel and existing systems coexist and share, in a centralised or decentralised way, resources, data and actions. As a result, novel services are enabled, and efficiency is increased. However, the nature of this context makes it difficult to trust fully on the goodness of the whole system, as multiple vulnerabilities are born mainly because of its complexity and heterogeneity. Moreover, in this particular context, one of the most dangerous threats are advanced persistent threats, or APTs. Therefore, SADCIP looks towards improving the state of the art, trying to find the necessary tools to a) monitor the technical capacities of the operational elements in the field, and b) detect relative evidence that, if applicable, should be addressed through optimal proactive response systems [3].

> “Any novel scenario that implies open communication with the Internet will bring numerous security problems”

Javier Lopez

Prof. Javier Lopez is Full Professor in the Computer Science Department at the University of Malaga, and Head of the NICS Lab. His research activities are mainly focused on information security, future Internet security, and critical infrastructure protection, and has lead several international research projects in those areas. Prof. Lopez is Co-Editor in Chief of IJIS journal and the Spanish representative in the IFIP TC-11 on Security and Privacy Protection in Information Systems.

e-mail: jlm@lcc.uma.es


Mass Customization
Simulation
Cloud Computing
Big Data Analysis
Internet of Things
Assets Location in Real Time
Aditive Manufacturing
Modular and Self-Adapted Production Chain in Real Time
Autonomous and Collaborative Robotics
Augmented Reality and Predictive Maintenance

Some icons made by Freepik from www.flaticon.com

Figure 10: Scheme of an enhanced Industry 4.0 factory.

The threat of APTs

Nowadays, Industrial Control and Automation Systems have been affected by an increased number of inside and outside threats, mainly due to the interconnection of industrial environments with modern ICT technologies. Beyond traditional IT threats (e.g., malware, spyware, botnets), one major issue is the existence of Advanced Persistent Threats (APTs). They consist of a new class of emerging and sophisticated attacks that are executed by well-resourced adversaries over a long time period. By combining multiple attack vectors that include the exploitation of zero-day vulnerabilities, together with stealthy and evasive techniques [2], many APTs go undetected over time. Although APTs were used against military organisations in the first term, they are now targeting a wide range of companies, hence drawing the attention from researchers focused in the industrial security sector [4].

> “The flexibility and intelligence of Industry 4.0 factories comes at a cost: APTs will be able to influence over industrial processes in subtler ways.”

Stuxnet was the first attack of this kind, reported in 2009, which sabotaged the Iranian Nuclear Program by causing physical damage to the infrastructure and therefore slowing down the whole process for four years. Ever since, the number of reported vulnerabilities concerning the Industrial Control Systems has increased dramatically, as the research community has incremented its interest and new attacks have been disclosed: in total, 1309 vulnerabilities have been reported by ICS-CERT between 2010 and 2015 (see Figure 2 showing this growth [5]).

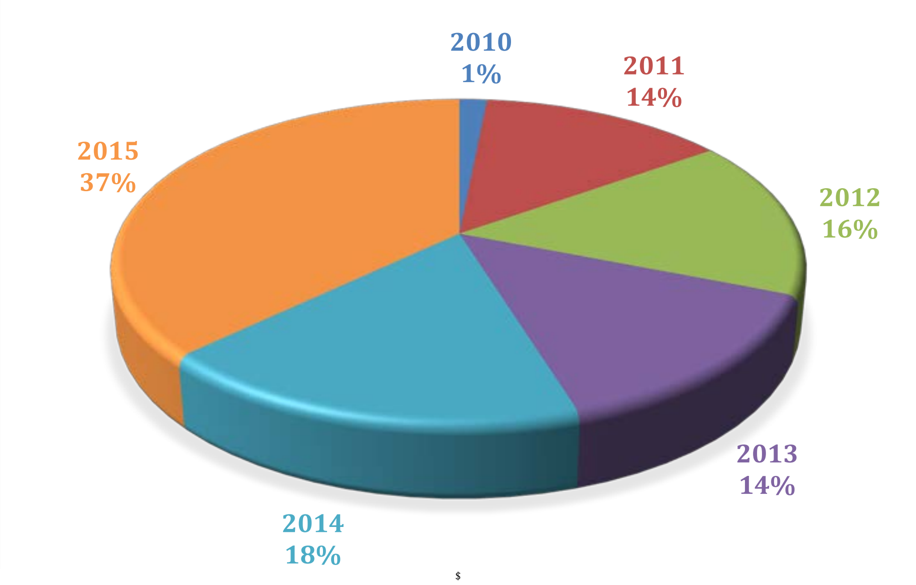


Figure 2: Reported vulnerabilities from ICS-CERT [5]

As Stuxnet, every APT follows multiple steps, beginning with an initial intrusion commonly using social engineering (e.g., by means of fraudulent e-mails containing Trojans). A successful intrusion results in the installation of a backdoor from which the attackers connect to the target network. Then, several exploits and malware are used to compromise as many computers in the victim network as possible (which is known as lateral movements), to ultimately modify the productive process or exfiltrate information back to the attacker domain. During the whole process, the threat actors make use of multiple tools to avoid detection and encrypt the external communication through publicly available services such as the Tor Anonymity Network.

Consequently, an additional effort is needed to mitigate the risks posed by these threats, which implies the effective detection of APTs through traditional countermeasures (e.g., intrusion detection systems, firewalls, antivirus) along with novel security services in continuous evolution within the company, involving all the organisation with effective security awareness training and gaining knowledge from old use cases. Numerous surveys show the evolution of awareness about this field in the industry. Specifically, we can highlight the ISACA Advanced Persistent Threat Awareness Study [6], carried on in July 2015, that provides a view of the APT perception from security professionals belonging to many industries, mostly technology services, financial, military, telecommunications and manufacturing companies. Among all the statistics, it is worth commenting an increment of 4 percentage points in security training and an increase in security budget in the 53% of the entities surveyed compared to 2014. Concerning the technical measures to protect against APT attacks, a very high percentage of those enterprises (95 percent) report that they are using antivirus and traditional network perimeter technologies (e.g., firewalls), while they increasingly leverage a variety of preventive, detective and investigative controls to help reduce the likelihood of a successful APT breach. This includes mechanisms like critical controls for mobile devices, remote access technologies (RATs) or sandboxing.

Industry 4.0 and APTs

The industry as a whole is aware of the problems posed by persistent attacks, and there are already various mechanisms that aim to facilitate their detection. Yet the solutions that are used in traditional industrial control and automation systems are not directly applicable to Industry 4.0 contexts. The integration of Industry 4.0 principles, such as interoperability, decentralisation, service oriented management, and interactivity, will fundamentally change all aspects of the industry: from the collaboration among supply chain partners, to the interactions between operators and machinery at the factory floor [7]. Yet it will also exacerbate the risks associated to APTs.

On the short term, industrial protocols like IO-Link and OPC UA will facilitate the interaction between existing and novel services. These and other technologies, like the Internet of Things, recognition services, and location services, will allow all individuals – from operators to administrators and executives – to access any relevant information anywhere at any time, helping them to make better decisions. Yet this interconnected ecosystem not only increases the attack surface, but also expands the influence that an APT can have in all actors once it has infiltrated into the system.

The deployment of open integrated factories and the integration of intelligent, dynamic processes are some of the medium and long-terms goals of the Industry 4.0, respectively. Such goals will enable the creation of flexible workflows and production processes, the deployment of intelligent assistants using novel HMI interfaces (e.g. wearables, augmented reality), and the advent of novel services such as the “digital twins” (maintenance and management through simulation), amongst other benefits. Yet this flexibility and intelligence comes at a cost: APTs will be able to influence over the behaviour of factory processes in subtler ways.

Moreover, we also should consider how the Industry 4.0 and the Internet will be closely linked. Beyond the use of IoT devices, and the convergence of IT/OT infrastructures, there are novel approaches, such as cloud manufacturing, that will allow traditional manufacturing components to become virtualised and deployed in the cloud. These novel approaches will be surely become a target of APTs.

SADCIP Project Goals

Given the effect that APTs will have over present and future Industry 4.0 deployments, it is essential to understand the potential risks and to develop an integrated solution that can effectively detect and react against APTs. Therefore, the specific goals of the SADCIP (Advanced System for the Detection of Persistent Cyberattacks in Industry 4.0) Project [8], which is funded by the Spanish Ministry of Economy, Industry and Competitiveness, are as follows:

- Analyse and investigate the characteristics of the most relevant cyber-attacks for Industry 4.0 environments.
- Develop security guidelines for Industry 4.0 environments, which not only serve to design safer infrastructures, but also to deploy defence mechanisms in a more optimal way.
- Create the basic components of a modular, flexible and easily adaptable intrusion detection architecture for Industry 4.0 scenarios, capable of cooperatively monitoring the existence of cyber-attacks that affect its fundamental elements (IoT, cloud / fog).
- Design and develop various transversal services that support the various elements of the detection system, including security services such as trust management systems, fog-based control services, etc.
- Develop relevant analysers for industry 4.0 environments, including scanners capable of detecting the lateral and data exfiltration attempts associated with APTs movements. These analysers will be platform agnostic, allowing their integration with other systems beyond the SADCIP architecture,

The proposed architecture and analysers are being developed in conjunction with the project coordinator, S2Grupo: a Spanish cybersecurity firm specialised in the development and integration of security solutions against APTs. In order to validate the results, these components will be integrated and validated in a testbed, where multiple attacks will be launched. Moreover, this testbed will also serve as a demonstrator of the resulting product.

References

[1] J. Wan, H. Cai and K. Zhou, “Industrie 4.0: Enabling technologies”, Proceedings of 2015 International Conference on Intelligent Computing and Internet of Things, Harbin, pp. 135-140, 2015.

[2] L. Cazorla, C. Alcaraz, and J. Lopez, "Cyber Stealth Attacks in Critical Information Infrastructures", In IEEE Systems Journal, issue 99, IEEE, pp. 1-15, 2016.

[3] C. Alcaraz, L. Cazorla, and J. Lopez, "Cyber-Physical Systems for Wide-Area Situational Awareness", In Cyber-Physical Systems: Foundations, Principles and Applications, no. Intelligent Data-Centric Systems, Academic Press, pp. 305 - 317, 2017.

[4] P. Chen, L. Desmet, C. Huygens. “A study on advanced persistent threats”. In IFIP International Conference on Communications and Multimedia Security, pp. 63-72, September 2014.

[5] ICS-CERT. Year in Review 2015. https://ics-cert.us-cert.gov

[6] ISACA. Advanced Persistent Threat Awareness Study Results. http://www.isaca.org

[7] J. Smit, S. Kreutzer, C. Moeller, M. Carlberg. “Industry 4.0”. European Parliament, Directorate General for Internal Policies, February 2016.

[8] SADCIP project, UMA, Spain. https://www.nics.uma.es/projects/sadcip

Authors’ Contributions

Prof. Javier Lopez is the principal co-investigator of the SADCIP project, and is in charge of studying the specific security challenges of Industry 4.0 scenarios.

Cristina Alcaraz

Cristina is an Assistant Professor at the Comp. Science Department of the University of Malaga. She is involved in all aspects related to detection and reaction of APTs in Industry 4.0 environments.

Jesus Rodriguez

Jesus is a computer science engineer working at the University of Malaga. He is analysing and developing the protection mechanisms for Industry 4.0 environments that will be applied in the SADCIP project.

Rodrigo Roman

Rodrigo is a Ph.D. researcher at the University of Malaga. He is studying the architecture of SADCIP, and analysing the protection mechanisms of IoT-services for the Industry 4.0.

Juan Enrique Rubio

Juan Enrique is a PhD Student in the University of Malaga. His main research includes the design and implementation of security services in the context of Industrial Control Networks and the Smart Grid.

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

Effective Defence against Zero-day Exploits Using Bayesian Networks

The goal of the work is to develop a Bayesian Networks based approach to maximise the system tolerance against zero-day attacks. A case study about ICS security management is demonstrated.

We investigate the possibility of improving the tolerance of Industrial Control Systems (ICS) against zero-day attacks by defending against known weaknesses of the system. We propose a metric to measure the system tolerance against zero-day attacks. We apply this metric to evaluate different defensive plans to decide the most effective combinations of available controls that maximise the system tolerance. A case on ICS security management is demonstrated in this paper.

Industrial Control Systems (ICS) play a crucial role in controlling industrial processes. Cyber security of ICS has increasingly become an urgent problem, owing to the wide use of insecure-by-design legacy systems in ICS and the physical damage of breached ICS to plants, and human health. Zero-day exploits (i.e. unknown exploits) have demonstrated their essential contributions to causing such damage by *Stuxnet*. The threat from zero-day exploits is still on the rise, but little effort has been done to combat them, because they are often unknown to the vendor.

Proposed Approach

It is extremely difficult to detect and defend against zero-day exploits. Sophisticated hackers are able to discover zero-day exploits before the vendors become aware of them. We consider the problem from a novel perspective, by seeking a way to make ICS sufficiently robust against zero-day attacks.

As shown in Fig. 1, a typical APT attack targeting ICS has to exploit a chain of vulnerabilities at different hosts to eventually breach the control devices (e.g. PLCs). The involved exploits use either known or zero-day vulnerabilities to propagate across the network. Whilst we can hardly defend against the exploitation of zero-day vulnerabilities, we can alternatively deploy effective defences against the known vulnerabilities such that the risk of the whole attack chain being exploited can be overall reduced.

A key attribute "exploitability" of weaknesses is borrowed from CWE to reflect the sophistication of a zero-day weakness. Weaknesses with higher exploitability are likely to cause higher risk. With regard to an acceptable level of risk, we define the tolerance against a zero-day weakness by the minimal required exploitability of the weakness to cause the system risk exceed the acceptable level. By using Bayesian Networks, we can prove that defending against known weaknesses is able to increase the tolerance, and find out the defence that maximizes the tolerance.

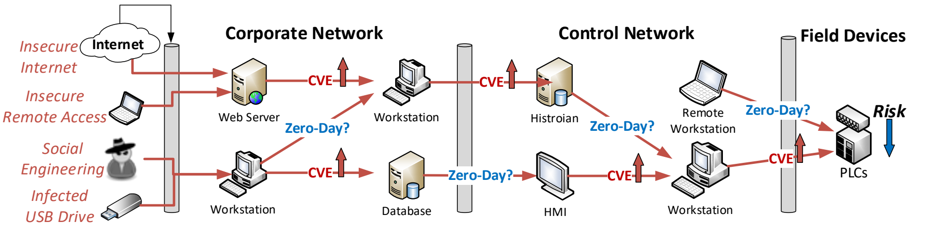


Figure 1: Multi-step Vulnerability-based Propagation across a typical three-zone ICS

Tingting Li

Dr. Tingting Li is currently a Research Associate at the Institute for Security Science & Technology, Imperial College London. She is working on the project *Research Institute in Trustworthy Industrial Control Systems (RITICS)* which mainly focuses on producing models and tools in support of effective defence for protecting ICS from cyber attacks. She obtained her PhD degree in Artificial Intelligence from University of Bath in 2014. She also received her MSc degree in Computing (Imperial College London, 2009) and her Bachelor degree in Information Security (Xidian University, China, 2008). Her research primarily lie in cyber security for ICS, logic-based knowledge representation and reasoning, multi-agent systems and agent-based modelling.

Email: **tingting.li@imperial.ac.uk**
https://www.doc.ic.ac.uk/~tl308/

Problem Modelling

We formally use Bayesian Networks (BN) to model ICS-targeted attacks with zero-day exploits involved and evaluate the risk. A discrete random variable is captured by a chance node in BN with a finite set of mutually exclusive states and a conditional probability distribution over the states. We further defined three types of chance nodes for different purposes: (i) *target nodes* indicate valuable assets in ICS with a set of known and zero-day weaknesses, (ii) *attack nodes* captures available attack methods between a pair of targets, and (iii) *requirement nodes* are designed to model particular objectives for evaluation. A *Bayesian Risk Network* is established based on the three types of nodes, where complete attack paths are modelled by target and attack nodes, and the damage of successful attacks are evaluated against requirement nodes.

We build a Bayesian network at the level of assets and model multiple weaknesses between a pair of assets by a single attack node, rather than multiple attack edges. Each attack node hence becomes a decision-making point for attackers to choose a (known or zero-day) weakness to proceed. Such Bayesian networks enable us to model zero-day exploits without knowing details about them (e.g. prerequisites or post-conditions), but focus on analysing the risk caused by zero-day exploits.

A defence control is able to reduce the exploitability of its combating weaknesses to certain degree subject to the effectiveness of the control. We select a particular node *N* to define the risk κ, which could be a valuable target node or a critical requirement. Thus κ is defined by the likelihood of *N* being compromised or violated, e.g. the likelihood of a requirement being violated must be less than 30%. The presence of a zero-day exploit at any target is likely to increase the likelihood as its exploitability increases. Thus, we define the tolerance by the minimum required exploitability of a zero-day exploit at each target to violate κ, or alternatively the maximum exploitability of a zero-day exploit the system can tolerate subject to κ.

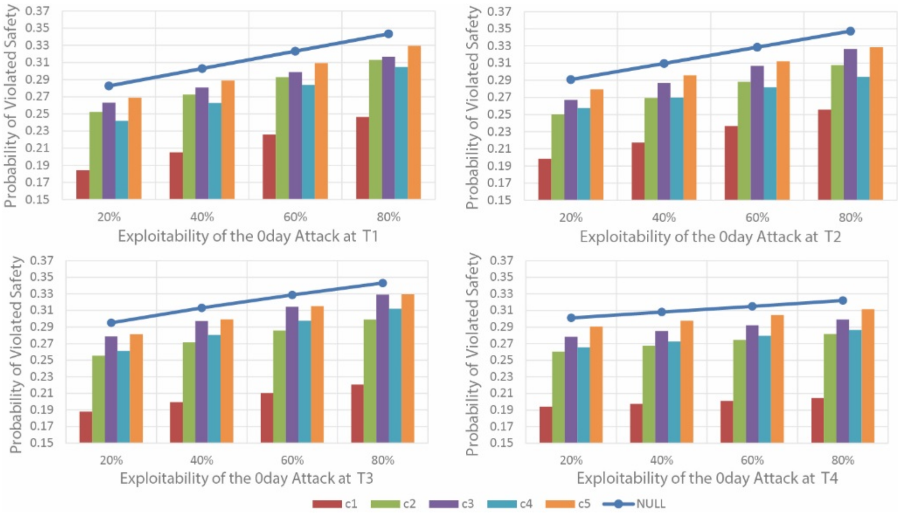


Figure 2. Risk distribution by single controls on each target with a 0day exploit

ICS Security Management

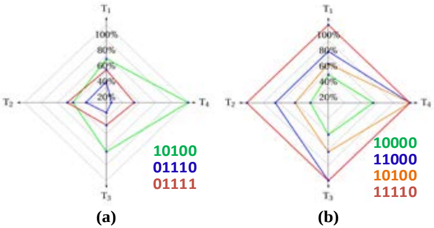
We used a hypothetical example to demonstrate our approach. A simple network is constructed consisting of common types of assets in ICS – a HMI, a workstation, a PLC and a RTU. The four assets are modelled as four target nodes *{T1, T2, T3, T4}* of a Bayesian network. We also selected five common weaknesses *{w1, w2, w3, w4, w5}* and five controls *{c1, c2, c3, c4, c5}* from the *ICS Top 10 Threats and Countermeasures*. These weaknesses are attached to relevant attack nodes between a pair of targets. In this case study, we consistently convert different levels of the CWE attribute "*Likelihood of Exploit*" into certain values. For instance, weaknesses that are identified as "*Very High*" by CWE are set to *0.8*

To model the cyber-physical effects of potential exploits, we consider three key requirements in the example. We use the likelihood of violating the requirement on *control availability* to measure the *risk* in this example.

Results

We construct the corresponding *Bayesian Risk Network* for the case study, and run four trials of the experiment in each of which a zero-day exploit is added to each target. In each trial, different defence controls are individually deployed and the updated risks over scaled exploitabilities of the zero-day exploit (e.g. *20%, 40%, 60%* and *80%*) are computed. In the four charts of Fig.2, the upper curve with markers illustrates the trend of the risk with none control. The mitigated risk by deploying each control are indicated by the coloured bars respectively.

The existence of zero-day exploits generally increases the risk. The zero-day at *T2* is the most threatening one as it brings the greatest increment to the risk, while that at *T4* is the least threatening one. This is because *T2* influences more subsequent nodes than *T4*. The control *c1* is the most effective one to reduce the risk. The tolerance against zero-day has been improved by deploying controls. From Fig.2, at least a zero-day exploit with exploitability *31%* is needed at *T2* to reach the critical level. By applying *c2*, a zero-day exploit with much higher exploitability *74%* at T2 is required to reach the same level of risk.



(a)

(b)

Figure 3: Zero-day Tolerance Coverage

In addition to applying single controls, we also run experiments to find out the most effective combinations of controls (i.e. defence plans). We use *bit vectors* to represent including or excluding a control in a plan. For instance, a plan *10011* indicates to apply *c1, c4* and *c5*. We looked at the impact of each plan on the maximal risk when the zero-day exploit at each target reaches its maximal exploitability, the risk reduction over different targets and tolerance.

We convert the tolerance value at each target into a radar chart as shown in Fig.3. From the Fig.3 (a), we can see that deploying more controls does not always guarantee a larger tolerance coverage. Each control combats different weaknesses that are distributed over different nodes. Defending against more widespread weaknesses would generally produce more risk reduction across the network. Besides, weaknesses near the attack origin tend to have greater impact on the risk of all subsequent nodes, and hence applying defences against earlier attacks are relatively more effective. The tolerances against a zero-day exploit at four targets are expanded at various rates. From the Fig.3 (b), the zero-day exploit at *T4* seems to be the easiest one to be defended, while *T1* and *T2* are the most difficult ones. Three out of the four plans in Fig.3 (b) make the system immune from the zero-day exploit at T4, but only *11110* can protect the system from the zero-day at *T1* and T2.

CYCA 2016

This work was accepted as a regular research paper at the 11th International Conference on Critical Information Infrastructure Security (CRITIS 2016), and presented in the CYCA session at Union Internationale des Chemins de fer (UIC) in Paris.

Tingting was very fortunate to be awarded the CIPRNet Young CRITIS Award (CYCA). We are sincerely grateful to have received this recognition from CIPRNet.

Collaborator

This work was collaborating with Prof. Chris Hankin. Prof. Hankin is Director of the Institute for Security Science and Technology and a Professor of Computing Science at Imperial College London. He was Deputy Principal of the Faculty of Engineering from September 2006 until October 2008. He was Pro Rector (Research) from June 2004 until September 2006. He was Dean of City and Guilds College from 2000-2003. His research is in theoretical computer science, cyber security and data analytics. He leads multidisciplinary projects on developing advanced visual analytics and providing better decision support to defend against cyber attacks.

He is Director of the CPNI/EPSRC Research Institute on Trustworthy Industrial Control Systems (RITICS). He is the immediate past President of the Scientific Council of INRIA, the French national institute for research in computer science and control. He is Chair of the Academic Resilience and Security Community (Academic RiSC) and sits on the ministerial oversight group of the Security and Resilience Growth Partnership and the steering group of the Home Office Security Innovation & Demonstration Centre.

Research Institute in Trustworthy Industrial Control Systems (RITICS)

This work is supported by Research Institute on Trustworthy Industrial Control Systems (RITICS), co-funded by EPSRC and CPNI (EP/L021013/1). The research project is coordinating with other four universalities in the UK: City University, University of Birmingham, Lancaster University and Queen's University Belfast.

Originally designed as isolated networks, ICS have evolved to become increasingly interconnected with IT systems and other, wider, networks and services – particularly as the technologies needed to deliver all manner of computing tasks have converged and proliferated. Whilst offering great efficiencies in terms of setup and running costs this trend has exposed ICS to a growing range of vulnerabilities and the potential for large inter-organisational impacts.

In recognition of these trends *RITICS@Imperial* focuses on five key areas: 1) Investigating the level of connectedness in different scales of organisations to understand the complexity of network topology and interconnections between critical infrastructures; 2) Conducting quantitative studies on the likeliest propagation paths of potential attacks; 3) Predicting ongoing persistent attacks; 4) Evaluating economic consequences of threats for various scales of organisations including an analysis of a loss of key assets and reputation; 5) Finding the most effective interventions to mitigate the risks for ICS.

If you would like to know more about RITICS please visit our website: http://www.ritics.org

If you would like to access this publication and other related publication, please visit Tingting's University profile: https://www.doc.ic.ac.uk/~tl308/

If you would like to know more about the Institute for Security Science and Technology at Imperial College London, please visit our homepage: http://www.imperial.ac.uk/security-institute

Figure 4: CYCA award ceremony at CRITIS 2016.

This page is intentionally empty.

Ensuring Network Security for Critical Information Infrastructures

Network Security and Resiliency

Network Security

Many critical information infrastructures encompass multi-site connectivity. Metropolitan Area (MAN) and Wide Area Network (WAN) security is deployed at the edge of each site. A viable solution must provide network security and resiliency. This requires overall security and resilience, encompassing device, data plane, control plane and management plane.

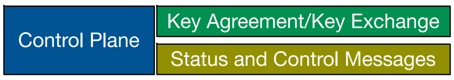
A single weakness in one of those four areas will compromise security and resiliency. A secure device is the foundation. Dedicated network encryption appliances can provide the level of security and resilience required for critical information infrastructures. Multi-purpose solutions embedded in network appliances and virtual appliances tend to fail to provide a secure and resilient device.

Data Plane Security and Resiliency

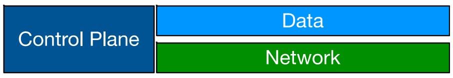
The data plane carries the network traffic that travels between the sites. This traffic should be encrypted using authenticated encryption with additional authenticated data. AES-GCM with a key size of 256 bit can provide the desired security. Line rate encryption/decryption and forwarding even at small frame/packet sizes (64 bytes) is mandatory to maintain network performance and ensure resiliency against denial-of-service attacks. As multi-site networks are static, a regular change of the session key (data encryption key) is required. AES-GCM uses a counter and for any key a counter state can only be used once. Session key changes must take place without interrupting the network traffic. To protect the network against traffic flow analysis, traffic flow security can be added to the data plane to obfuscate the actual network traffic. There are two different approaches to traffic flow security: (1) Using uniform frame/packet sizes, and (2) injecting synthetic network traffic into the traffic flow. Uniform frame/packet sizes have a negative impact on latency and overhead. Moreover, the supported use case is often limited to point-to-point connections. The injection of synthetic network traffic has a negligible impact on latency and overhead, especially if used in combination with frame/packet grouping, and it can support all network topologies. This method is challenging in terms of making the synthetically injected traffic look indistinguishable. Nevertheless, there is an increasing preference and demand for this approach.

Control Plane Security and Resilience

With most of the focus of network encryption being on the data plane security and resilience, it is easy to overlook the importance of the control plane security and resilience. Data plane encryption requires keys and these are provided over the control plane.



Key agreement, key exchange and the transmission of status and control messages must be properly protected to ensure proper operation of the data plane security mechanisms. A successful attack on the control plane will disrupt the network encryption or even the entire network.



This mandates a resiliency against denial-of-service attacks, which can only be provided by direct line-rate

Christoph Jaggi

Christoph Jaggi works as technology, strategy and marketing consultant.

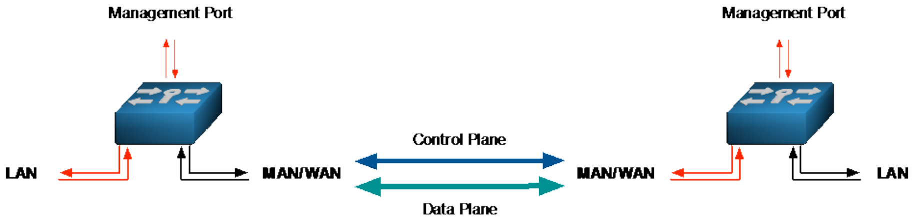
e-mail: cjaggi@uebermeister.com

http://www.uebermeisster.com

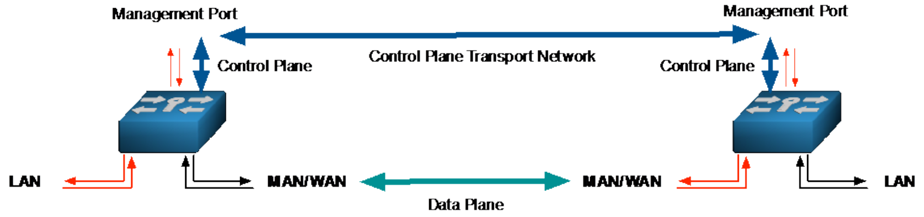
More detailed information is available on the author's website. (see the end of this article)

hardware support for the control plane encryption at the network layer used for the transport of the control plane. Otherwise the result is a cryptographically sound solution that can be easily disrupted.

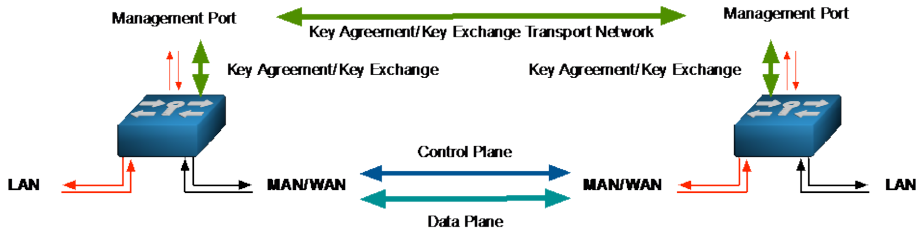
The control plane can be transported in-band together with the data plane. The session key used for the control plane should be different from the key used for the data plane and it must not be the same key as the key encryption key used for encrypting the data during the key exchange.



In some environments it is preferred to separate the transport network for the key agreement/key exchange from the transport network used for the data plane. There are two scenarios: (1) The entire control plane is transported over a separate network, and (2) only the key agreement/key exchange is transported over a separate network, while the status and control messages use the same transport network as the data plane.



The dedicated management port of the encryption appliance is used to hand over the entire control plane or the key agreement/key exchange to the management section of the LAN. Network security and resilience for the transport are provided by an encryption appliance that acts as gateway to the transport network used for the control plane or the key agreement/key exchange. From a security and resilience point of view it makes only sense to separate data plane and control plane, if the security and resilience provided on the alternative transport network is equal or higher than the one provided by the encryption appliance for the data and control plane.


Management Port
Key Agreement/Key Exchange Transport Network
Management Port
Key Agreement/Key Exchange
Key Agreement/Key Exchange
Control Plane
LAN
MAN/WAN
Data Plane
MAN/WAN
LAN

Management Plane

Access to device management must be restricted to the management port. Different access methods use their own private and public keys, such as SSH. Overall security is compromised if the different access methods are not properly secured or if the different management roles are not properly separated.

Using COTS (commercial off-the-shelf) Equipment

Custom-built high-assurance solutions that are certified for "confidential", "secret" and "top secret" tend to come at a high price and suffer from limited availability due to low production volumes, high development cost, high evaluation cost and limited export permissions. They also tend to be engineered for a limited number of scenarios. For most critical information infrastructures, commercial off-the-shelf (COTS) equipment can provide the required protection level at a much lower price point and with much better availability; but only if the COTS equipment fulfils the extended security requirements. Such equipment is normally evaluated and certified for government use for information classified as "restricted". Some of the COTS equipment fulfils the requirements for "confidential" and can be used for such environments if the national authorities agree to such use, even if the basic approval of the equipment is limited to "restricted".

COTS Equipment, Evaluations, Certifications and Approvals

Using COTS equipment for network security can be in many cases a viable option for securing critical information infrastructure. It is however a challenge to find and select a solution that provides the network security and resilience needed for critical information infrastructures. This is caused by the different evaluation, certification and approval requirements and processes. FIPS has issues in terms of the evaluation as overall US security requirements are lower than in some other countries, the evaluation does not go into such detail as source code analysis and security architecture. The evaluation is limited to the cryptographic algorithms and to the cryptographic modules. The latter can be part of a system and thus be dependent on the overall security of such a system. This results in security incidents affecting products that use FIPS-certified cryptographic modules. It is important to take a close look at the evaluation reports for a product to understand what has been evaluated and certified before deciding to use such a product. The result are security incidents affecting products that are FIPS-certified.

For the transport of classified data with a low classification level the U.S. National Security Agency (NSA) thus proposes to use a double encryption (inner and outer tunnel) on different layers when using COTS equipment for multi-site connectivity. The assumption is, that even if the security provided by one COTS equipment is insufficient, the use of a second COTS equipment for adding another layer of encryption could compensate for it. This is only necessary if the COTS equipment used does not provide the required security level and it does not guarantee that the required security level is actually achieved. This approach also has a noticeable impact on latency and overhead. It is much wiser to use COTS equipment that provides the required security levels without needing a second layer of encryption at network level. The German BSI and other national information security agencies use this approach, as it is more cost-efficient and much better suited for networks. A Common Criteria evaluation and certification depends on the profile that is used for the evaluation and the evaluation level. The evaluation depth of profiles can differ substantially. There is at least one US profile for network encryption that equals security and device boundary and makes the assumption that the device is secure. To properly assess the value of a Common Criteria certification it is therefore necessary to look at the profile used, the depth of the evaluation and the detailed test report.

Links to in-depth background:

www.uebermeister.com/files/inside-it/2014_Introduction_Encryption_Metro_and_Carrier_Ethernet.pdf
www.uebermeister.com/files/inside-it/2014_Evaluation_Guide_Encryptors_Carrier_and_Metro_Ethernet.pdf
www.uebermeister.com/files/inside-it/2015_market_overview_Ethernet_encryptors_for_Metro_and_Carrier_Ethernet.pdf

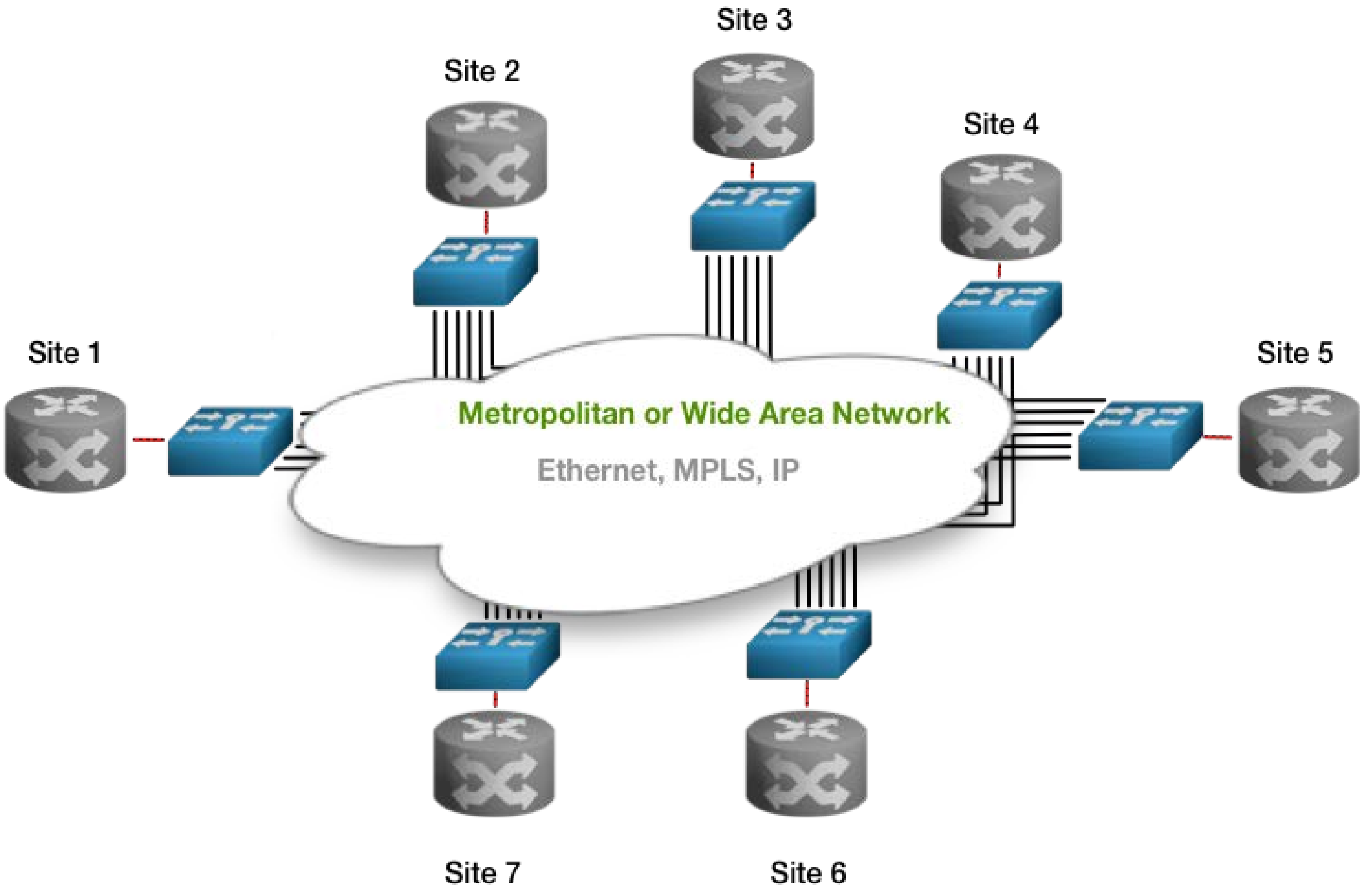


Figure: Multisite Connectivity MAN-WAN

This page is intentionally empty.

A taxonomy of tools for CI Security Testing

Critical Infrastructure Security Testing must not be overlooked.

Introduction

The fundamental objective of Critical Infrastructure Protection is the development, implementation or enhancement of Security, both in its physical and logical / cybernetic aspects since they are both inherent master pieces of such systems, as it is represented in Figure 1. In particular, the management of Cybersecurity of the components of Infrastructures, (equipment, networks and systems in which the information is logged), whether critical or not, is a fundamental task. It is therefore fundamental the identification and valuation of assets of an organisation, the identification of threats and vulnerabilities, the estimation of their frequency of occurrence and associated impacts, for the calculation of risks that both individual devices and Industrial Control networks as a whole can suffer. In this sense, it has to be taken into account that the concept of Security of the information systems that support these infrastructures has, as main objective, to guarantee its reliability. Particularly, control automation & supervision, the integrity of the information handled, and the availability of such systems.

This focus leaves in the background aspects such as those related to confidentiality of information (which, on the other hand, they must be observed carefully in particular scenarios (e.g., telemetering and remote management.)

SCADA (Supervisory Control And Data Acquisition) is a software system capable of communicating with different devices and exercising actions on them from a management panel. This software allows control from industrial automation networks to manage and interpret telemetries belonging to machines in production.

The diversity and convenience provided by SCADA software has spread its use in the industrial field, being its role to control most of the critical infrastructures of the countries.

As in less critical systems, the fact that a software is in charge of the management of most relevant assets, makes it an appetizing target for cybercriminals or adversary governments. The first known Advanced Persistent Threat (Stuxnet) was directed against the SCADA system of an Iranian nuclear enrichment plant and gained control of its system through the monitoring and manipulation of plant’s processes.

Despite Stuxnet demonstrated that such type of critical systems is vulnerable, there are still in place SCADA systems that remain exploitable. The reason is that traditionally, the administrators of this type of systems believed that they were secure because the systems were not connected to the internet and their code was kept internally hidden. This belief also released them from applying proper security mechanisms. Fortunately, nowadays the “security by obscurity” principle is defeated by Kerckhoff's second principle, i.e., "The security of the system should not depend on its design being a secret." Moreover, the uttermost importance of the security of national critical infrastructures is recognised such that is mentioned, for instance, in the Cyber

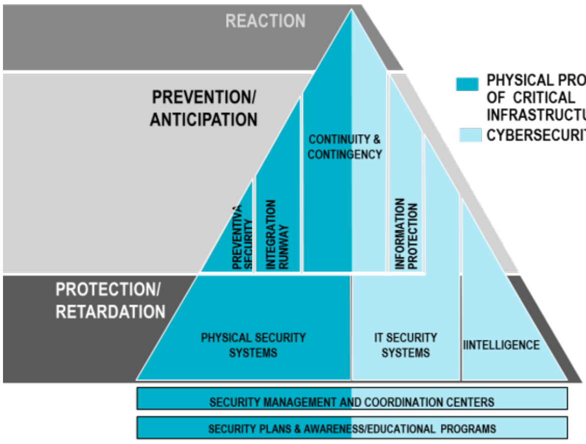


Fig 11.CI Physical & Logical Security sides

Marina Egea

Dr. Marina Egea is the Head of the Tiger Team, Cybersecurity Operations at Minsait (by Indra).

e-mail: msegea@minsait.com

Luis Miguel Cerrato (left)

is Cybersecurity Analyst in the Tiger Team at Minsait, and GCIH, GIAC Certified Incident Handler.

Jose Boix a (right)
is in favor of offensive security is a security analyst of the Tiger Team of Minsait (Indra)

Alejandro Espinosa)

is a Cybersecurity Analyst of the Tiger Team of Minsait (Indra)

Defence pledge published by NATO after the Varsovia summit in 2016.[1]

In this paper, we focus on highlighting the importance of the logical security of SCADA systems and how it can be tested. In particular, we provide a taxonomy of existing tools to perform penetration tests on SCADA systems. We do not intend to build here an exhaustive list but, at least, to differentiate those analysis tools which are SCADA-specific from those "usually employed" security testing tools which are still valid to perform pentesting tasks for SCADA systems.

Selected tools have been classified according to the following categories:
- Information gathering
- Traffic analysis
- Vulnerability scanning
- Vulnerability exploitation

Also, we have included Linux distributions which are oriented to help testing the security of SCADA systems.

In the following sections, we will first describe the different components that are usually found in SCADA systems. Then, we will explain the different categories of tools that exist and their role in the context of a pentesting process.

SCADA components

In order to understand what is involved in a pentesting process of a SCADA system, we describe here briefly its conceptual components.
SCADA systems allow to transmit individual device status, manages energy consumption by controlling devices, allow direct control of power system equipment and even chemical plant processes, oil and gas pipelines, electrical generation and transmission equipment, manufacturing facilities, etc.

A SCADA system usually has the following components:

- SCADA WorkStation: which is a device operated by a human operator that allows to command a central SCADA console.
- HMI (Human-Machine Interface): It's usually a piece of software and hardware that allows the human operator to monitor the state of the processes which are under control, to modify control settings, manually override auto-control operations, etc. Namely, the HMI is the human-friendly interface that provides access to the SCADA workstation.
- Data Historian: This component is in charge of gathering and storing information from the system with the aim of facilitating accurate post-analysis.
- SCADA Server MTU (Master Terminal UNIT): This component is a device that issues the commands to the Remote Terminal Units (RTUs) which are located at remote places from the control so as it can gather the information that is distributed, processes and displays it.
- RTU (Remote Terminal Units): These are the connecting sensors which report or actuate according to the local information that they obtain from the supervisory systems.
- PLC (Programmable Logic Controller): This component automatically performs the main site control process which controls the operation of industrial equipment.

The SCADA server MTU and the RTU or PLCs are in communication through specific SCADA protocols. The main ones are i) DNP3 (Distributed Network Protocol)[2] used for communications between the MTU and RTU through port 20000 TCP/UDP; and ii) ModBUS[3] which is typically used for SCADA-style network communication between devices implementations over serial TCP/IP (standard port 502 TCP). In a nutshell, RTU collects data from sensors which sends to the MTP using either DNP3 or ModBus protocols. The main drawback of these protocols is that they were not designed having security in mind (no authentication, no encryption, no validation).

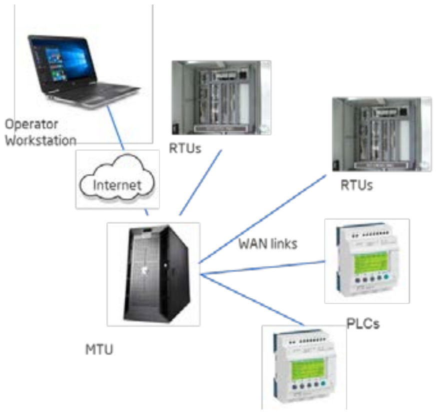


Figure 12. SCADA Industrial Control System Concept

Attack vectors for SCADA systems

Once we have described the conceptual architecture of a SCADA system, we will review some attacks vectors that may impact such architecture.
Taking into account the weakest link in the security chain, we have to say that Administrators and Operators many often have very few security knowledges.
From SCADA protocol descriptions we infer that SCADA systems share the same threats to any other TCP/IP-based system. Also, we have to mention that PLCs and RTUs usually use vendor-specific network and protocols.
Since many SCADA systems are incorporating web application interfaces to allow remote access by administrators, widely known web vulnerabilities must be considered. Thus, some of the following attacks which particularly affect to availability and integrity of the systems might succeed:

- Denial of Service against the MTU, RTU or PLCs.
- SQL injections to delete or modify data history, which would lead to loss of operations.
- Infect the system with a piece of malware, e.g., a Trojan to take control or spy the behaviour or industrial sensitive information of the system.
- Vulnerabilities known on communication protocols including non-secure design or wireless communications vulnerabilities, e.g., negotiated keys or full communication hijacking.
- Exploit commonly known web vulnerabilities[4]
- Scan the network topology and associated technologies to search for non-updated operating systems, open ports, etc.

In summary, we need to be aware that at the end of the day we are

[1] http://www.nato.int/cps/en/natohq/official_texts_133177.htm

[2] https://standards.ieee.org/findstds/standard/1815-2012.html

[3] http://www.modbus.org/specs.php

[4] https://www.owasp.org/index.php/Top_10_2013-Top_10

dealing with devices, operating systems, protocols over TCP, databases and firewalls. It is known that security mechanisms to mitigate known weaknesses already exist, however, the deployment of these mechanisms in SCADA architectures is not always that feasible.

Pentesting tools for SCADA systems

The phases of a pentesting for a SCADA system are the same that are used for any other IT system. We illustrate them in Figure 3 (starting with the Information gathering phase).

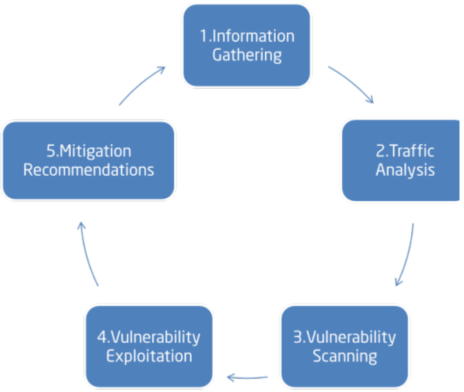


Figure 13. Pentesting phases

1. Information gathering

The aim of this phase is to gain as much information as possible about the target system.

- **Shodan:** Many control panels of SCADA systems are connected to the internet to allow remote control. Remote control is very convenient for system administrators, but opens an attack vector that can be exploited to manipulate the system. Shodan is a search engine capable of finding systems exposed on the internet, performing a comprehensive scan and indexing of the information. It permits to know if a system is exposed to the Internet being classified as vulnerable. Shodan offers a very versatile API that is exploited by cybercriminals through bots, able to re-compile the information needed to later perform brute force attacks. In order to determine that a system on which a pentesting is to be performed is safe, the first thing to check is whether the system appears in Shodan and if the access to it is vulnerable. [https://www.shodan.io]

- **ZoomEye ICS:** ZoomEye is a search engine that allows grabbing data from publicly exposed devices and web services. The ZoomEye ICS is mainly focused on finding ICS (Industrial Control System). It offers the chance to perform easy custom searches based on a list of protocols and products available. Moreover, more specific searches can be performed through its web or with its public API. Search filters are available to get accurate results, like application, software, product, version, device, Operating System, country or IP, among others. [http://ics.zoomeye.org]

- **Nmap:** Nmap is an open source tool for network discovery and services and ports scanning. Each open port is a possible access to the system, hence a port scanning is a technique commonly performed by any attacker who want to exploit a system (not only a SCADA system). [https://nmap.org/]

    - **ICScanner:** ICScanner is a tool used for enumeration of devices on SCADA network environments. It supports reconnaissance of many SCADA protocols, i.e. Modbus serial, Modbus TCP, DNP 3, Profinet, Siemens SIMATIC Step 7, etc.. [https://github.com/0xICF/ICScanner]

    - **PLCScan:** PLCScan is a tool that allows scanning PLC devices over s7comm or Modbus protocols.

      [http://www.digitalbond.com/tools/plcscan/]

2. Traffic analysis

The main goal of traffic analysis in a pentesting process is to identify certain patterns after getting information about the network flow.

- **Wireshark:** Wireshark is a network protocol analyser. It allows live monitoring and saving traffic captures for further analysis. Wireshark functionality in SCADA traffic analysis can be increased through the use of plugins like Siemens s7 Wireshark dissector. [https://sourceforge.net/projects/s7commwireshark/, https://www.wireshark.org/]

- **Scapy:** Scapy is a packet manipulation program, available as a Python library as well as a CLI (Command Line Interface). It allows any kind of operation with network packets, even at bit-level. Useful for industrial environments thanks to its capability of working with custom, specific protocols. Feature that makes it especially suitable for the analysis of SCADAs' protocols. [http://www.secdev.org/projects/scapy/]

3. Vulnerability scanning

Vulnerability scanning is performed to identify operating systems, services and vulnerabilities present on a target system. Several commercial and open source scanners allow scanning SCADA systems in order to identify certain vulnerabilities.

- **Nessus:** Nessus is a cross platform vulnerability scanner. It is a commercial tool that checks whether a system is vulnerable or not through a set of plugins written in NASL (Nessus Attack Scripting Language). Reports can be generated following the severity of the vulnerabilities found. [https://www.tenable.com/products/nessus-vulnerability-scanner]

- **OpenVAS:** OpenVAS (Open Vulnerability Assessment System) is an open source framework of services and tools used for vulnerability scanning and vulnerability management. Given that OpenVAS is a fork of Nessus, some similarities exist between them. OpenVAS checks if a target is vulnerable through a scanning using a set of plugins written in NASL. After the scan has finished, the vulnerabilities are classified by its severity. **[http://www.openvas.org/]**

- **Splonebox:** Splonebox is an open source network assessment tool. One of its main features is the availability of custom plugins, including some specific to analyse industrial communication protocols. [https://splone.com/sploneb ox/]

Vulnerability exploitation

- **SCADA Shutdown Tool:** It allows the pentesters to detect and interpret all the controllers of the system and later modify their registers in order to explore the limits of the system. [https://github.com/0xICF/SCADA ShutdownTool]

- **PLCinject**: With the PLCinject tool you can enter code inside the devices commonly known as PLCs. One can test if they can be altered by certain vulnerabilities. [https://github.com/SCADACS/PL Cinject]

- **Metasploit**: Metasploit is an open source penetration testing software. It is written in Ruby and gives multiple options for different phases of a pentesting, not only for the vulnerability exploitation phase. Its modularity is a great advantage given that different modules can be added to increase its functionality. In terms of SCADA exploitation, a set of modules have been developed to take advantage of vulnerabilities in different products and vendors. [https://www.metasploit.com]

- **SCADAPASS:** It allows brute-force attacks on SCADA systems based on dictionaries containing commonly used default passwords. Although the security of these systems is critical, it is surprisingly often to find weak or default passwords protecting the access. [https://github.com/scadastrange love/SCADAPASS]

Linux pentesting distributions (SCADA oriented)

Although a number of tools exist to support a pentesting process, configuring them properly for a SCADA system is not an easy task. Because of this reason tailored pentesting distributions for SCADA systems were created. The main ones are:

- **Moki Linux:** a distribution of pentesting tools to analyse SCADA systems. It can be used to extend Kali Linux OS, so it is not necessary to install an extra operating system.
- **Quickdraw:** SCADA Snort Rules.
- **PLC Scan:** PLC scanning tool.
- **CoDeSys exploit:** Remote buffer overflow exploit for CoDeSys Scada web-server.
- **Modscan:** Application designed to operate as a MODBUS Master device.
- **Siemens s7 metasploit:** Auxiliary module of metasploit for Siemens S7
- **Siemens s7 wireshark dissector:** plugin for Wireshark to detect Siemens S7 traffic

[https://github.com/moki-ics/moki]

- **SamuraiSTFU:** it is the most famous distribution for pentesting on SCADA. It includes a great set of tools and it is capable of emulating SCADA systems so that a laboratory for testing purposes can be created. [http://www.samuraistfu.org/]

After reviewing these phases and tools, we notice that, in summary, for SCADA systems we can audit:

- Network Infrastructure: router configurations, switch tables, DNS tables, traffic analysis.
- Host operating systems: version, patch level, password strength, authentication and authorisation policies, and access points.
- Applications: ports and services, remote access, protocols.
- For PLCs and RTUs: Review patch levels, password quality, packet sniffing (incl. wireless). Check whether physical attacks are possible.
-

Conclusions

Traditional approaches to “security by obscurity” in SCADA systems are not sufficient to protect this type of systems nowadays. Especially since common hacking techniques can be employed to attack these systems, as we have reviewed in this article. In order to ensure a good level of security in SCADA systems, the following mechanisms should be taken into account:

- Network segmentation or the creation of DMZs to separate privilege levels, access to data, etc.
- Robust communication protocols.
- Firewalls properly configured and without making dangerous exceptions (as often we find while auditing systems).
- Proxy serves to mediate between the traffic originated in the internet and internal traffic.
- Effective security policies which coordinate physical and logical security as well as management of systems by the operators.

Security training for the staff who needs to operate the system which is essential for preventing attacks or the materialisation of misuse cases.

iHoney Project: New concepts in honeypot development for ICS cybersecurity

The ever-increasing need for a realistic honeypot calls for a two-sided approach: IT and OT Engineers working together.

Abstract

Honeypots are an important tool that can be deployed for critical infrastructure protection. In addition to this, intelligence gathered from realistic honeypots exposed to the Internet is a useful input for the development of specific security capabilities. IT and OT systems present relevant differences that have to be accounted for when designing, implementing, deploying and running an ICS honeypot. This article focuses on these specific issues and presents the results of the research carried out by the S2 Grupo ICS Security team, highlighting the basic principles and the insights gained from the iHoney R&D project.

Introduction

Many critical infrastructures (CI) depend on industrial control systems (ICS) for their normal operation. ICS security is, thus, becoming a major concern in critical infrastructure protection (CIP). Since Stuxnet was reported in 2010 [1], ICS Security has evolved into a brand new field for cyber security companies and the rest of the stakeholders. As such, a new body of knowledge and tools (software, hardware...) suitable for industrial environments are being developed and deployed. There are two basic requirements that such a tool should meet:

- Use of technical auditing software should not, under any circumstances, disturb or disrupt the regular operation of the infrastructure in which it has been deployed. Limits to this requirement shall be determined by the owner of the IC assets.
- When talking of cyber security monitoring systems (i.e. IDS/IPS) this requirement should be extended to guarantee that the equipment and network connections deployed for monitoring purposes do not weaken the security perimeter by opening new vectors in de CI, even if the probes are compromised by malware or attackers.

However, for the time being, most of the tools available in the market are a mere application of the IT cyber security methodologies, practices and software into the ICS environment. This is the result of a state of mind that regards ICS as a bunch of IT components, failing to grasp the essential point: even if these systems are becoming more and more similar to standard IT environments (Linux/windows OS, TCP/IP communications, servers, workstations, etc.), the people behind and the way they are operated by them are totally different.

So we need new tools to be developed specifically for ICS protection, and this can only be accomplished with sound knowledge of this field, as well as with a clear awareness of IT/OT differences. This has been the main objective of the iHoney project, which also included the development of an ICS honeypot as a means of gathering first-hand information on the kind of threads a CI is exposed to. This has shown to be a valuable source of intelligence on: typology of attacks, frequency, strategies, tools... which in turn has complemented the experience and knowledge of the interdisciplinary team of process, security and communications engineers that have been involved in the project.

The honeypot is one of the project's most innovative milestones, because beyond the immediate practical applications summed up in the aforementioned purposes, its development has been intended to provide an answer to the following questions:

- Who is interested in causing damage to a CI? How many of these individuals/organisations are out there?
- Do they have the skills and motivation required to perform successful attacks?
- What are their goals?
- And, above all:

Oscar Navarro

Óscar Navarro is an electrical engineer. He has a wide experience in SCADA and ICS systems and worked for engineering and construction companies before joining S2 Grupo. Currently he leads the S2 Grupo ICS cybersecurity team.
He is an expert in anomaly detection in SCADA systems and ICS security management.

e-mail: onavarro@s2grupo.es

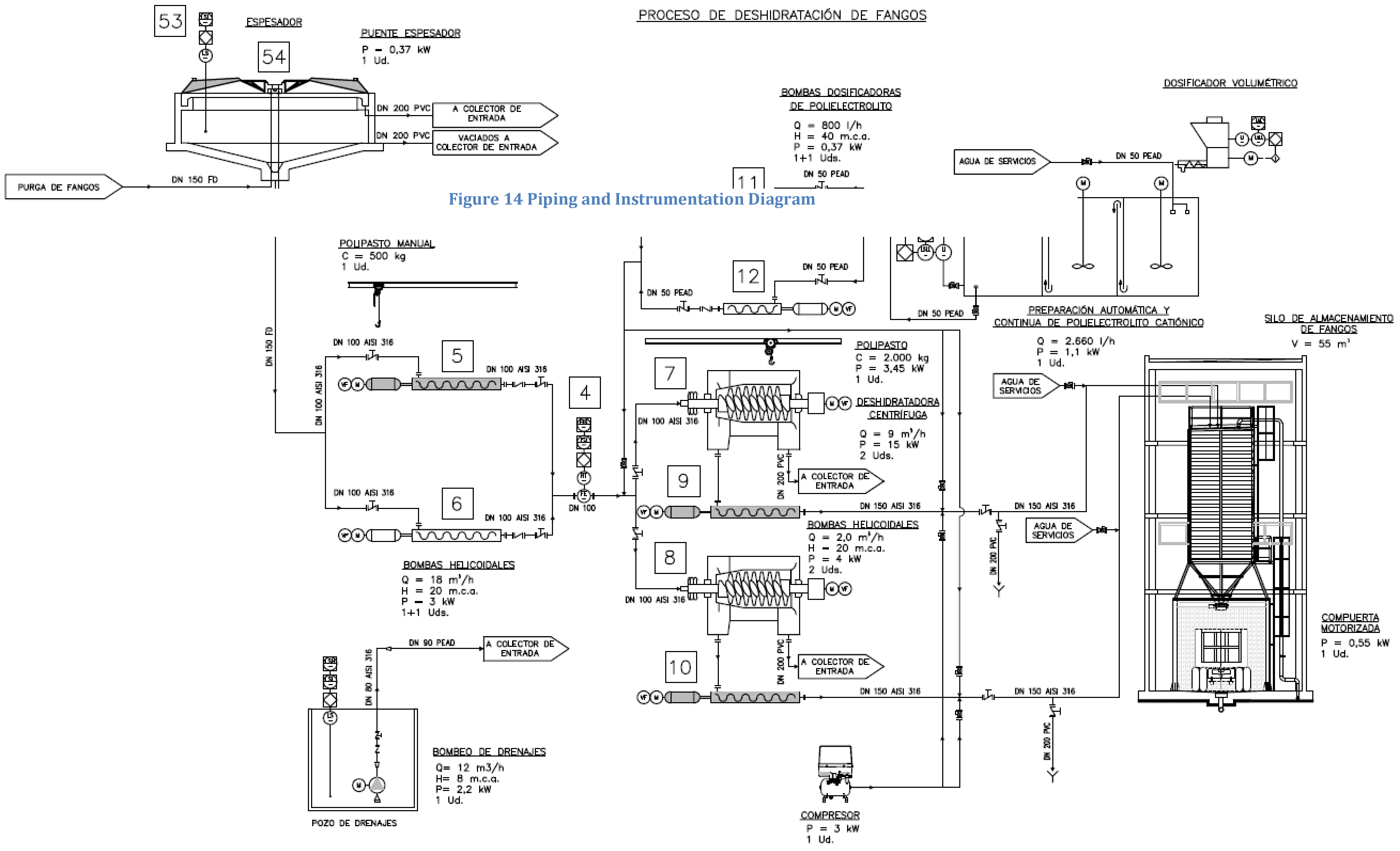


Figure 14 Piping and Instrumentation Diagram

Do they have skills and knowledge on ICS (design, operation, etc.) good enough so as to plan and execute sophisticated attacks resulting in damage for physical equipment and processes?

Building a realistic honeypot

A review of the state-of-the-art of ICS honeypots carried out during the initial phases of the project (see for example [2]), showed that there were common pitfalls that should be avoided right from the start. A brief list of the most relevant among them follows:

- ICS honeypots tend to be over-simplistic when it comes to industrial processes. The reviewed cases didn't match any realistic process and, what's more, consisted only in software simulations running in a computer which had some common ICS protocols ports open.
- Physical equipment was lacking or scarce. A typical configuration was that of a single PLC (Programmable Logic Controller) communicating with a computer.
- Typically, ICS honeypots are too simplistic to allow any complex interaction with a potential attacker, thus preventing any sophisticated actions from taking place.
- A tendency to over-promote the honeypot on the Internet as a means to enhance its visibility and attract attackers, complemented with just too evident vulnerabilities put in place 'to let the bad guys in'.

Summing up: Attackers with a sound knowledge on industrial processes and ICS technology are not likely to be deceived by the reviewed honeypots, which look far too much IT-inspired. The most probable 'victims' of these honeypots are casual or conventional attackers, biasing the data on malicious activity obtained in this way.

In order to answer the questions asked above, a brand-new approach is required. So, right from the onset of the design activities, some important basic premises were stated:

- The simulated infrastructure must be a realistic one, comparable to those a modern society relies upon.
- The honeypot must be realistic enough so as not to raise suspicion, not only in casual or IT aimed attackers, but also in personnel with experience in ICS and industrial processes.
- The honeypot must allow for a degree of interaction high enough for complex attacks to take place. More precisely: in order to keep an attacker engaged for as long as possible, the system must show some kind of response to malicious actions. In fact, this action/reaction pair should match reality as close as possible. For example, if an attacker expects, as a result of his actions, a pump to stop, flow through the corresponding pipe should drop to zero smoothly, just as the real thing would do.
- Contrary to IT honeypots, cyber security monitoring must be almost invisible. The reason is that currently most SCADA systems lack complex monitoring infrastructures and an attacker would find an IDS in operation suspicious.

The iHoney honeypot (*i* stands for *industrial*) has been designed, built and operated on these principles. The project was planned and executed just as the ICS for an actual infrastructure would have been. The main milestones were:

1. Fake infrastructure design. For this project, a water treatment plant was selected. The design involved treatment process definition and associated calculations, equipment selection (pumps, blowers, instrumentation...). Summing up: all the requirements to design an actual plant like the one selected.
2. Automation and ICS system design: controllers, communication buses and protocols, architecture, etc.
3. Graphic interface development for the SCADA HMI interface (Human-Machine Interface). This task was carried out in a realistic manner because of the blueprints already designed in the previous phase. In addition to the plant layout, other common screens were also developed: alarms, historian, etc.
4. Physical processes modelling by means of logical and mathematical expressions that involve the considered state variables. This is the core of the process simulator.
5. Cyber security monitoring subsystem design: architecture, software, communication networks, connection to the Internet, etc. A set of hardware and software was deployed for monitoring purposes. By employing S2 Grupo CERT technology, generated alerts were directed towards the CERT to be managed by S2 Grupo specialists.
6. ICS system implementation. ICS hardware was deployed and programmed as an actual system would have been. This task was accomplished with help from a specialised contractor.

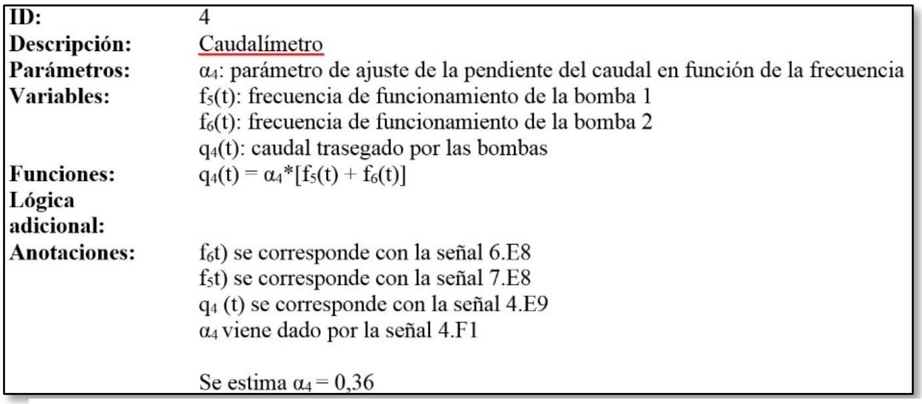
So, the iHoney ICS honeypot consists of three differentiated modules:

- The ICS system, composed of an SCADA server/HMI, a control network of PLC that regulates the several processes and the associated industrial communication protocols.
- The simulation system, that evaluates the process status variables in real-time and interacts with the ICS inputs (legitimate or not) generating the appropriate outputs (as the actual system would). This system provides 'plant operators' with an interface that enables them to interact with the physical system: physical buttons and switches to operate manually, drives and panels, local interfaces to manually change setpoints, etc.
- The cyber security monitoring infrastructure.

Overcoming challenges

During the project execution, some important issues have required special attention. Here follows a list of the most relevant:

- Some compromises were necessary to ensure, on the one hand, a realistic enough fake system and, on the other hand, an adequate level of complexity. So some simplification has been made in the mathematical relations between physical variables. Of course, there is a limit to this imposed by the need to keep the system simple but realistic.
- Choosing an infrastructure prone to be cyber-attacked. This is kind of a goldilocks problem: attractive enough but not so notorious that it raises suspicion. For example, choosing a big airport may not be such a good idea as it seems: it is difficult to simulate in a realistic manner; it is not likely that serious attackers take a singular infrastructure overexposed on the internet for the real thing; the possible impact of a casual attack on such a notorious thing may dissuade most individuals.



ID:	4
Descripción:	Caudalímetro
Parámetros:	α_4: parámetro de ajuste de la pendiente del caudal en función de la frecuencia
Variables:	$f_5(t)$: frecuencia de funcionamiento de la bomba 1 $f_6(t)$: frecuencia de funcionamiento de la bomba 2 $q_4(t)$: caudal trasegado por las bombas
Funciones:	$q_4(t) = \alpha_4*[f_5(t) + f_6(t)]$
Lógica adicional:	
Anotaciones:	f_6t) se corresponde con la señal 6.E8 f_5t) se corresponde con la señal 7.E8 q_4 (t) se corresponde con la señal 4.E9 α_4 viene dado por la señal 4.F1 Se estima $\alpha_4 = 0{,}36$

Figure 2: Mathematic modeling function example

- Implementing the honeypot so as to render the simulation module invisible. One of the key factors to achieve this is the use of 24 V DC signals in the communication between the ICS and the simulating module.
- Simulating the response of physically driven relays built in some actual equipment (for example, overheat emergency switches in submersible pumps) and safety interlocks.
- Developing a high-quality set of layout blueprints as a template for the SCADA HMI interfaces.
- Integrating the simulation module and the ICS one accounting for the tight requirements of ICS systems regarding real time processing, stability and network latency.
- Customizing the monitoring system to conceal the generation and exfiltration of information on attacks (logs, etc.)

Once the design and construction stages were over, the iHoney honeypot entered the operational phase. A maintenance and operation plan was designed that included activities such as:

- Scheduled maintenance stops.
- Scheduled operations (on a daily, weekly and monthly basis).
- Scheduled equipment failure simulation.

This plan was put in place to keep the infrastructure 'alive', as any potential attacker would expect from an actual plant.

Lessons learned

The iHoney was exposed to the Internet for over 1.5 years while S2 Grupo ICS cyber security team detected, analysed and recorded all the malicious activity taking place in the system.

When the operational phase was over, a thorough analysis of the compiled data was carried out, and in fact, is still in progress. However, some important lessons learned can be highlighted:

- Most of the registered attacks are automated and are directed against the IT components of the SCADA system. Now that Industry 4.0 is the new paradigm, and it is becoming harder to draw a line between IT and ICS systems, the cyber security of these systems must be approached globally.
- When properly configured and updated, it is not easy for attackers to get into the system. So, the importance of a good security management can hardly be overstated. In fact, this is prompting attackers to explore other ways in, such as social engineering (see next paragraph).
- The iHoney project was strongly technology-oriented. However, a certain number of attacks were directed against the operators behind the machines. Since human operators are the weakest link in the cyber security chain, this is a factor that any future (ICS) honeypot must account for. iHoney is very realistic from a technical point of view, but lacks the corporate and human components. This is an important insight for future experiences.

References

[1] *Gregg Keizer, "Is Stuxnet the 'best' malware ever?". InfoWorld, 16 September 2010.* *http://www.infoworld.com/article/2626009/malware/is-stuxnet-the--best--malware-ever-.html*

[2] *Kyle Wilhoit. "Who's Really Attacking Your ICS Equipment?". TrendMicro, 2013.* *https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/white-papers/wp-whos-really-attacking-your-ics-equipment.pdf*

.

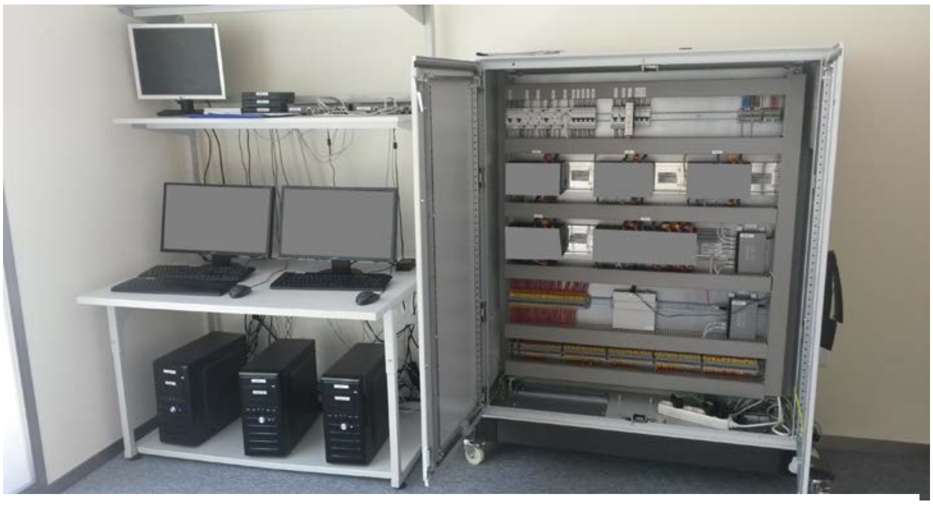


Figure 3: SCADA real equipment

CRITIS 2016: Conference Highlights

The 11th International Conference on Critical Information Infrastructures Security (CRITIS) took place in Paris, France, on 10–12 October 2016

The 11th International Conference on Critical Information Infrastructures Security (CRITIS 2016) was held at UIC Headquarters, Paris, from 10 to 12 October 2016.

The conference was organised by the International Union of Railways (UIC) with co-chairing support from Campus Bio-Medico University of Rome (UCBM) and Ecole des Ingénieurs de la Ville de Paris (EIVP). The conference provided a global forum for constructive exchanges between experts from governments, regulators, scientists, academics, service providers, and other stakeholders on topics concerning Critical Information Infrastructure Security and Critical Infrastructure Protection at large.

10-12 October 2016
UIC HQ Paris, France
CRITIS
2016
11th International Conference on Critical Information Infrastructures Security

Key figures

CRITIS 2016 marked the beginning of the second decade of CRITIS. The participants and speakers came from fourteen European countries (Belgium, France, Germany, Italy, Lithuania, Luxemburg, Portugal, Romania, Russia, Slovenia, Spain, Switzerland, the Netherlands, United Kingdom) and six countries from other continents: Morocco, Japan, Singapore, South Africa, South Korea, and USA. The conference participants had the opportunity to enjoy an excellent technical program, at UIC Headquarters, in the very heart of Paris, between the banks of the Seine and Champs de Mars, only a foot away from the Eiffel Tower.

Following the call for papers, we received 58 high-quality submissions, which were thoroughly reviewed by the expert members of the International Programme Committee (IPC). Out of the total submissions, 22 papers were accepted as full papers with eight further papers accepted as short papers offering work in progress.

Programme summary

The 2.5-day technical programme consisted of 30 papers grouped into sessions that included topics on: innovative responses for the protection of cyber-physical systems, procedures and organisational aspects in C(I)IP and advances in Human Factors, decision support, and cross-sector C(I)IP approaches.

As in previous years, invited keynote speakers and special events complemented the technical programme. The four keynote interventions were the following:

Dr Arturas PETKUS (NATO Energy Security Centre of Excellence, NATO ENSEC COE, Lithuania) talked about CEIP and Energy Security in Perspective of NATO (CIPRNet Lecture) see https://enseccoe.org/en .

Commander Cyril STYLIANIDIS (Ministry of Interior, General Directorate for Civil Protection and Crisis Management, France) provided an overview of "The Crisis Interministerial Cell (CIC), the French tool for interministerial level crisis management", illustrated with recent examples from France.

Mr Kris CHRISTMANN (University of Huddersfield, Applied Criminology Centre, UK) gave an overview of the "Findings from the PRE-EMPT Project: Establishing Best Practice for

Grigore M. Havârneanu

Traffic and Transport Psychologist with a PhD in Social Psychology. Research Advisor within the International Union of Railways' Security Division

Programme Chair of CRITIS 2016 and new member of the CRITIS Conferences Series Steering Committee

e-mail: **havarneanu@uic.org**
www.critis2016.org

Reducing Serious Crime and Terrorism at Multi-Modal Passenger Terminals (MMPT)".

Dr Paul THERON (Thales Communications & Security, France) presented "A way towards a fully bridged European certification of IACS cybersecurity", related to the work of DG JRC's ERNCIP Thematic Group on IACS cybersecurity certification.

The PDF files of the presentations can be found on the CRITIS2016 website:

www.critis2016.org/programme

Furthermore, in continuation of an initiative first taken up at the 2014 CRITIS, the conference also included an award for young researchers in the area (the 3rd CIPRNet Young CRITIS Award), seeking to recognise and encourage the integration of talented younger researchers into the community. Six of the accepted papers were presented during a dedicated CYCA Session. The winners were Amalie Grangeat (CEA France) and Tingting Li (Imperial College London, UK). This award was sponsored by the FP7 Network of Excellence CIPRNet.

CRITIS 2014 and 2015 proceedings have been published in Springer LNCS 8985 and 9578 respectively.

CRITIS 2016 proceedings are currently with Editor aiming for a release in Springer LNCS in the second quarter of 2017.

In addition, some of the CRITIS 2016 participants had the opportunity to attend (within the limited number of places) an associated event organised at UIC the next day after CRITIS. The IMPROVER Workshop: "Meeting public expectations in response to crises" – addressed an important topic in C(I)IP, aiming to discuss how infrastructure operators meet these requirements today and how this can be improved.

Acknowledgements

It is our pleasure to express our gratitude to everybody that contributed to the success of CRITIS 2016. In particular, we would like to thank the General Chair Jean-Pierre Loubinoux (UIC Director-General) and the local UIC hosts Jerzy Wisniewski (Fundamental Values Department Director) and Jacques Colliard (Head of UIC Security Division) for making CRITIS possible at UIC Headquarters in Paris.

Further, we would like to thank the members of the Programme Committee who did a tremendous job under strict time limitations during the review process. We also thank the CRITIS 2016 Co-Chairs Prof. Roberto Setola (UCBM, Italy) and Hypatia Nassopoulos (EIVP, France) and the members of the Steering Committee for the great effort and their continuous assistance in the organisation of the conference. We are also grateful to the Publicity Chair and to the UIC Communications Department for their excellent dissemination support, and to the CIPRNet Network which was an active supporting community.

We are equally grateful to the keynote speakers who accepted our invitation and agreed to round off the conference programme through presentations on hot topics of the moment.

Finally, we thank all the authors who submitted their work to CRITIS and who shared their new ideas and results with the community. We hope that these ideas will generate further new ideas and innovations for securing our critical infrastructures for the benefit of the whole society.

The next edition of the International Conference on Critical Information Infrastructures Security

CRITIS 2017

will be hosted in Lucca, Italy between 9 and 13 October, 2017

to continue the successful CRITIS conferences series.

www.critis2017.org

CRITIS 2017: 12th International Conference on Critical Information Infrastructures Security – Call for Papers

The 12th edition of CRITIS will take place at IMT in Lucca, Italy, October 9–13, 2017

In 2017, the International Conference on Critical Information Infrastructures Security will celebrate its 12th anniversary. This year edition continues the efforts to bring together scientist, experts, policy makers and professionals from academia, industry and govern-mental organisations engaged in the field of the security of critical (information) infrastructure systems.

As in previous editions, invited keynote speakers and special satellite events will complement a programme of original research and stakeholder contributions. The conference provides a bridge for the different research communities and disciplines involved in the C(I)IP while encouraging discussions, conceptualisations and modelling, especially when based on multi-disciplinary approaches.

CRITIS 2017 will push forward the tradition of presenting original research, whilst exploring new challenges in the field of critical (information) infrastructures protection (C(I)IP). To this purpose special efforts will be devoted to foster the dialogue with stakeholders and assess a common language and vision.

Conference Organisation

CRITIS 2017 will be organised according to six different topics which correspond to six virtual sessions.

CS “Cyber Security”: Modern society and especially the CI’s are experiencing continuous changes toward the smart paradigm. Each device is nowadays endowed by an intelligent controller while being part of a complex system controlled by sophisticated and increasing smart electronics. In other words, countries at elevated level of development are following a path toward the advent of “smart society”. Smart grids, smart water supply, smart cities do represent the eventual evolution of our present infrastructures. Recent attacks to CIs via the cyber side demonstrate how thin is the boundary between the cyber and the physical world. For these reasons, cyber security plays a central role in any complex human activity, especially in CIP. In particular, enhancing the cyber security of SCADA systems or designing and building intrinsic fault tolerant automated adaptive systems by new generation cyber controllers represent extremely interesting issues.

TR: Transports. Following the positive experience of the past edition at UIC, a specific session will be devoted to transports. Railways, highways and their integration represent one of the most dwelling subjects, both on the scientific and the technological sides. The increase automation of transports also raises specific issues concerning security. Similarly, due to deliberate hostile human activities such as terrorist attacks, vandalisms, thefts, etc, specific actions and protections need to be enforced.

Submission of papers:
June 2-nd 2017

Registration open:
July 1-st 2017

Acceptance Notification
July 15-th 2017

Camera-ready papers:
September 1-st 2017

CRITIS Conference
October 9/11-th 2017

CRITIS Satellite Workshops
October 12/13-th 2017

Antonio Scala CNR (left)
General Chair CRITIS 2017
Professor Institute of Advanced Studies IMT (Lucca)
e-mail: antonio.scala@cnr.it

Gregorio D’Agostino, ENEA (right)
Program General Chair
Lectutet at Univ. Roma II “TorVergata” and President Netonets Association (www.netonets.org).
gregorio.dagostino@enea.it

Programme Co-Chair:
Cristina ALCARAZ, Univ. Malaga
e-mail: alcaraz@lcc.uma.es

Grigore HAVARNEANU, Research Advisor, UIC Security Division
e-mail: havarneanu@uic.org

Poster Co-Chair:
Hypatia NASSOPOULOS, Ecole des Ingénieurs de la Ville de Paris
hypatia.nassopoulos@eivp-paris.fr

Local Co-Chairs:

Guido Caldarelli (left) full professor in Theoretical Physics at IMT

Rocco De Nicola full professsor Computer Science IMT Lucca

The IMT - Institute of Advanced Studies IMT (Lucca)
Is the main organizer of the Conference.
Meeting will be hosted in the ancient scenario of the San Francesco area: a gothic Complex built between the 14- and the 17-th centuries.

UR: Urban Resilience. The exploding human concentration in the urban areas, would be, on its own sake, a reason to devote a specific session to this significant subject. More importantly, urban areas do involve a huge number of different interdependent infrastructures that represent an un-paired scenario where to test modelling and managing capabilities developed insofar by the scientific community. One of the most delicate points is the cost/benefit analysis related to the allocation of redundant resources required to improve resilience. In particular, the security of smart buildings, smart districts and smart cities are requiring increasing efforts.

TIS: Trust Information Sharing is the elective paradigm that is commonly invoked to deploy any collaboration among different stakeholders. The creation of shared contingency plans and other forms of collaboration to deal with undesired events represent one of the most effective means to increase the global resilience of any system of systems. It is worth stressing that complex interdependent systems are not limited to the regional or national level, but may also involve cooperation at European or trans-border level. TIS is also at the basis of any Public-Private Partnership, which represents a promising means to improve preparedness, share the risk and handle contingencies.

HF: Human Factors. Modern infrastructures and their aggregations are exhibiting a constant trend toward automation. However, the humans will always continue to play an essential role in several respects. Decision makers will always be central while facing unpredicted contingencies. People behaviour as local operators and especially as customers and citizens can highly influence the resilience of the society both by collective un-reasonable (psycho-social) behaviours or by cooperative synergistic actions, or even by providing creative unplanned resilient solutions. Modelling and training of decision makers and population's behaviours represents one of the most advanced sectors of research performed by theoretical conceptualisations, realistic modelling and real gaming experiments.

EM: Emergency Management. Last but not least, this topic presents a great deal of efforts from both academic and applied sides.

Generally speaking, it is the most critical part of the Preparation Cycle. The Planning, the Early Warning, the Recovery Phase, the Optimisation of the residual resources, the coordination of different actors, are just some of the issues involved when facing a catastrophe or a crisis. Floods and earthquakes represent the most common hazards; specific works to face such events are solicited. Population awareness and the role of the media during crisis also represent significant issues.

The former scheme represents just a preliminary organisation of topics. However, all advances related to the resilience enhancement or assessment and the protection of human beings and our society are welcome; including new technologies to improve quality of life or preserve our historical heritage and natural environments.
Similarly, standalone studies on Modelling, Analysis and Simulation of CIs deserve special attention regardless of their application to any specific session above. In particular, emergent behaviours (such as financial crisis or psycho-social hysteresis) have been demonstrated to be a mere consequence of the complexity (systemic risk) of the systems, not of some specific characteristics. The same considerations apply for forensic issues and policy making and enforcements by authorities of any level, from mayors to European Deputy Members.

Conference Chairs and Organisers

Antonio Scala has been appointed general chair of the conference by the Critis Steering Committee. He combines experience in Interdependent Critical Infrastructures both at theoretical and applied level (especially in the Electric System). Due to their long-standing collaboration, Gregorio D'Agostino has been also involved as Program General Chair. Following the success of 2016 organisation and to insure continuity with the previous edition, last year cochairs have been confirmed, while further including Cristina Alcaraz.

Local organisers will be two outstanding full professors of the IMT hosting institution: Guido Caldarelli and Rocco De Nicola.

Critis 2017 novelties

The format of the conference has been preserved. However, some novelties have been introduced.

The **poster session** has been extended: about a third of the applications will be presented as a poster. The cloister of San Francesco complex in Lucca will host the event in an amasing environment.

YCA: Young Critis Award. Along the line of the CRITIS tradition, special attention will be devoted to young talents. To this purpose a prize will be awarded to the best contribution presented by a young author. During the last three years this prize has been supported by the CIPRNET European network of excellence (www.ciprnet.eu) and named CYCA (CIPRNET Young Critis Award); this year it will renamed generically YCA (Young Critis Award) and it will be organised in collaboration with the International Research Institute "Res on Network" (www.resonnetwok.it) and in particular with its Scientific Director Prof. **Marco Santarelli.** Three finalists will be selected based on their contributed abstracts and will present their work to the CRITIS audience, which will provide a second evaluation. Eventually a commission of academics and experts, chaired by Prof. **Bernhard Hämmerli**, will provide a third and conclusive evaluation to achieve the final response. Detailed rules for eligibility of candidates and evaluation procedure can be found on the CRITIS2017 web-site (www.critis2017.org/YCA.php).

Beside the main conference presentations there will be two **Satellite Workshops** on **Energy** and **Water**, respectively. This two workshops will take place on October 12-th and **13-th**. The workshop on Energy will be chaired by **Angelo Facchini** (IMT) and **Antonio Scala**, while the workshop on Water will be chaired by Angelo Facchini e **Gabriele Oliva** (University Campus BioMedico). Specific calls for contribution will be made available on the website for this satellite events.

Participants interested in Energy and Water issues are encouraged to participate to both the main conference and the specific workshops.

One of the aims of the CRITS series of conference is to provide a bridge between the Operators and experts from academy or research institutions. To this purpose a specific **"Operator Session"** is planned where Operators will present specific issues or their innovative solutions. It is worth stressing that, while the participation to this session does not require the submission of an abstract, nor the publication of any proceedings, the Operators may also participate to the conference as any other contributor.

To the purpose of providing a dissemination opportunity, a **"Project Session"** is also planned where each project on C(I)IP will be given the opportunity to present its state of the art, preliminary results and ongoing work.

Beside the planned satellite workshops, other events can be possibly hosted upon request. In this respect, Projects on CIP will be given the opportunity to organise their **dissemination events** during CRITIS conference.

Paper submission

We encourage submissions containing original ideas that are relevant to the scope of CRITIS 2017. Researchers are solicited to contribute to the conference by submitting research papers, work-in-progress reports, R&D project results, surveying works and industrial experiences describing significant advances in C(I)IP. Stakeholders from governments, Critical Infrastructure operators, and industry are encouraged to submit papers which describe their current and future challenges to be engaged by researchers and multidisciplinary research teams.

It is required that papers are not submitted simultaneously to any other conferences or publications; and that accepted papers not be subsequently published elsewhere. Papers describing work that was previously published in a peer-reviewed workshop are allowed, if the authors clearly describe what significant new content has been included.

All papers need to be written in English. There will be full papers and short papers. Full papers should be no longer than 12 pages, including bibliography and well-marked appendices. Short papers should be 4 to 6 pages long. Any submission needs to be explicitly marked as "full paper" or "short paper". A paper can be also marked as "Poster" in case, this form of presentation is preferred.

All paper submissions must contain a title, a short abstract, and a list of keywords. All submissions will be subjected to a thorough double blind review by at least three reviewers. The paper submissions should be anonymised and all author names, affiliations, acknowledgements, and obvious traceable references should be eliminated.

Paper submission will occur via the EasyChair conference system at the following url: "https://easychair.org/conferences/?conf=netonets2017". Submitted papers (in PDF or PostScript format) must be formatted using the template offered by Springer LNCS and be compliant with Springer's guidelines for authors.

CRITIS 2017 continues the "Young CRITIS Award" activities for fostering open-minded young talents. CIPRNET European Network of excellence cooperated and supported this activity, which this year will be continued in collaboration of Res on Network (www.resonnetwork.it) a European research Institute.

Acceptance policy

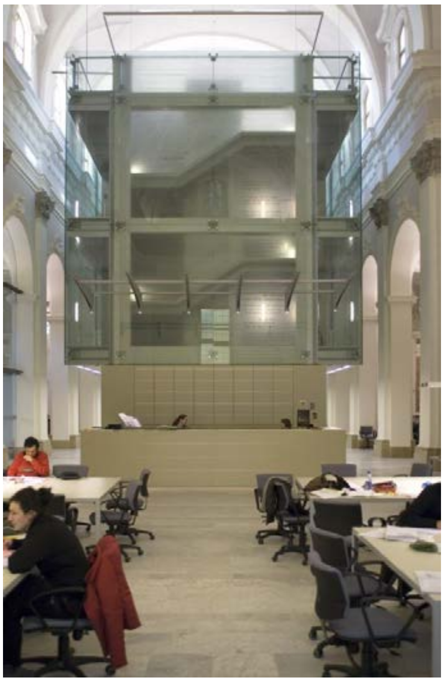
For publication in the CRITIS 2017 proceedings, all accepted oral papers (full and short) must be presented at the conference; at least one author of each accepted paper must register to the conference by the early date indicated by the organisers. Papers accepted as posters will not be published in the final proceeding, but will be included in the program and in the pre-proceedings.

The conference **pre-proceedings** will appear at the time of the conference. All accepted papers (including posters) will be included in full length in the pre-proceedings.

As in previous years, it is planned that **post-proceedings** are published by Springer-Verlag in their Lecture Notes in Computer Science (LNCS) series. Accepted full papers will be included in full length in the post-proceedings. However, we recommend that the authors produce a revised version of the paper, based on feedback received at the CRITIS event.

For accepted short papers, a four-page extended abstract will be included in the post-proceedings.
Any accepted paper (full paper and extended abstract) that shall be included in the post-proceedings requires that its authors sign Springer's copyright agreement.

Joining CRITIS 2017 In Lucca



Venue

CRITIS 2017 will take place at the IMT – School of advanced Studies premises, in San Francesco complex - Lucca.

Lucca is a renascent City grown on a roman original plant, which keeps its original walls intact. They are presently a pleasant pedestrian promenade. The city is overflown by churches and buildings of renaissance-era. Some of those buildings, including San Frediano Complex and San Francesco Complex have been donated to IMT which can now resort of a campus of about 10.000m2.

IMT Attractions: famous Library, hosted in San Frediano church, which represents a remarkable example of modern classical co-existence. For further information on IMT, please visit its web-site at https://www.imtlucca.it

More information

For further information on CRITIS 2017, lodging, travel directions, preliminary programme, etc., please visit the website at www.critis2017.org

Figure 15: The famous IMT Library in the former church of San Ponziano

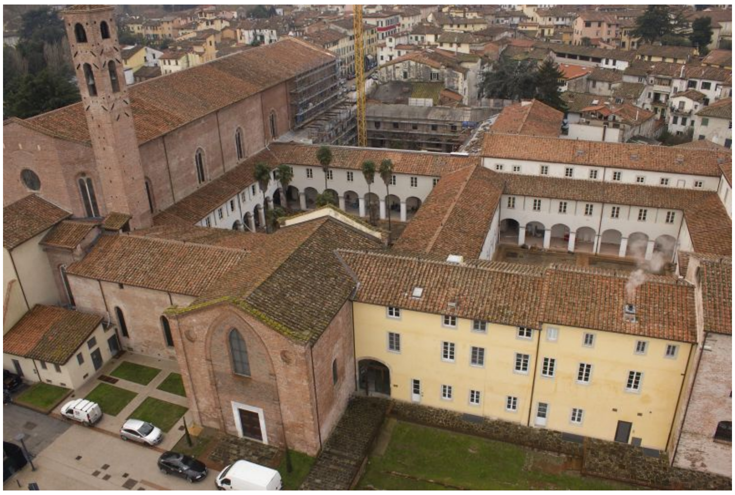


Figure 16: San Francesco historical complex, now part of the IMT premises (left)
Figure 3: Shah Italy - Lucca - view from Torre Guinigi (right)

See you at CRITIS 2017 in Lucca

www.critis2017.org

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

CRITIS 2017	www.critis2017.org	9-13 October, 2017, Lucca Italy

Institutions

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

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
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
Campus Bio-Medico di Roma	www.unicampus.it
EC Joint Research Centre	https://ec.europa.eu/jrc
Fraunhofer-Institut für Intelligente Analyse- und Informationssysteme IAIS	www.iais.fraunhofer.de
TNO	www.tno.nl/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 and a half years, CIPedia© reached 475,000 total views, at a current average of 480 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, CIPedia© 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.

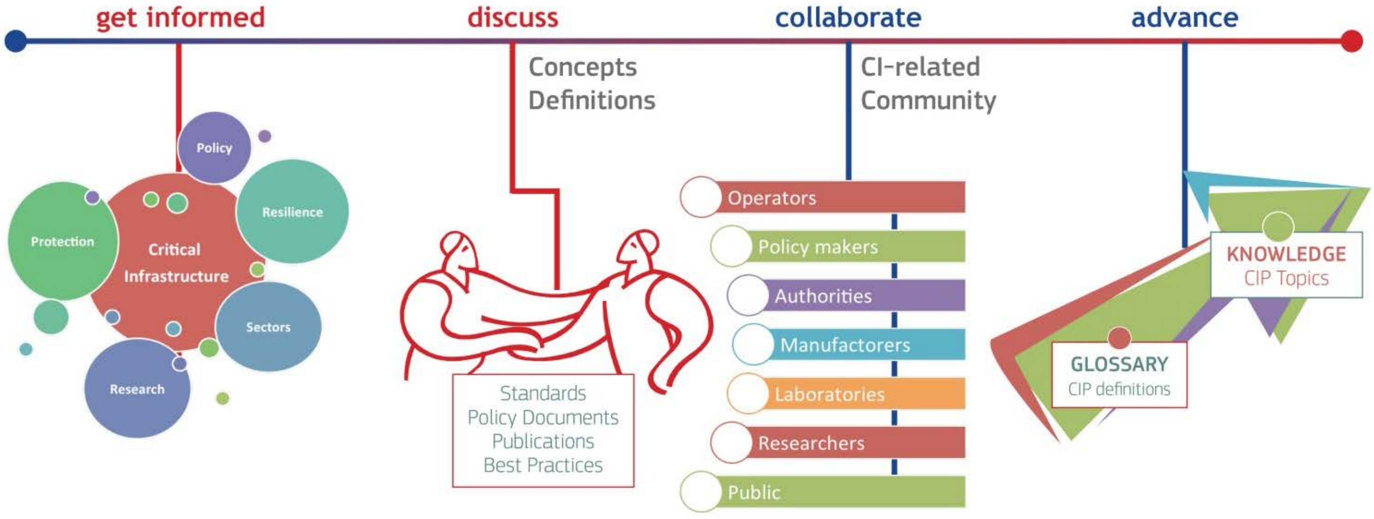
marianthi.theocharidou@jrc.ec.europa.eu

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.


get informed
discuss
collaborate
advance
Policy
Resilience
Protection
Critical Infrastructure
Sectors
Research
Concepts Definitions
Standards
Policy Documents
Publications
Best Practices
CI-related Community
Operators
Policy makers
Authorities
Manufactorers
Laboratories
Researchers
Public
KNOWLEDGE
CIP Topics
GLOSSARY
CIP definitions