Summary

Within the EU project CockpitCI "Cybersecurity on SCADA: risk prediction, analysis and reaction tools for Critical Infrastructure" and under the patronage of Étienne Schneider, Minister of Economy and Foreign Trade, itrust consulting and CREOS, organised the 3rd CockpitCI Workshop on "SCADA Cybersecurity" at Creos' national dispatching centre on March 10th, 2014.

This workshop enabled the European Union Agency for Network and Information Security ENISA, Luxembourgish authorities (Ministry of Economy, GOVCERT.LU, HCPN), the national electricity and gas operator CREOS and other Luxembourgish industrial attendees as well as the project partners to discuss problems and solutions on the security of critical infrastructures.

CockpitCI gave itrust consulting the opportunity to develop two software products: a meta anti-virus appliance called AVCaesar and a software version monitoring tool called Software Checker.

This article explains the context of Critical Infrastructure protection, the political ambition and practical risk to achieve this. Some results of CockpitCI are given, and a follow-up project, called Smart Grid Luxembourg Cockpit aiming to tailor security for the future network of smart electricity meter in Luxembourg is announced.

New security technology to face cyberattacks

CockpitCI: HOW TO MONITOR CYBERRISKS ON A CRITICAL INFRASTRUCTURE?

Dr Carlo Harpes, Matthieu AUBIGNY Ing.
itrust consulting s. à r. l.

1 Critical Infrastructure Protection

1.1 CI as target for attacks

Critical Infrastructures (CI) like electricity, gas or water distribution systems, and train or airplane controlling system are vital for the functioning of national and European organisations and industrial sectors. They should stay, at least partially operational, even in the event of serious dysfunctions due to natural disasters or malicious attacks. Nowadays, such infrastructures have become a target of cyber-attacks. The research experiment Aurora and recent attacks (Stuxnet, Duqu, Red October) have shown that all these networks and underlying industrial systems are potentially vulnerable to attacks. The Stuxnet malware ruined almost one-fifth of Iran's nuclear centrifuges, which are based on IT systems generally considered as well-protected, well segregated, and immune to cyber-attacks.

1.2 "Blackout"

The famous novel "Blackout" by Marc Elsberg describes the consequences of a cyber-attack shutting down the entire electrical supply of Europe. This fictional novel is based upon solid investigations on the functioning of the European electrical grid and its present vulnerabilities. The book describes the impossibility of detecting the causes and sources of the problem quickly enough, and it illustrates that the measures to prepare the population for the coming disaster have been insufficient.

1.3 The political aspects

Since 1990s, specific services have been considered as essential to maintain industrial activity in a country and even to ensure the way of live for its citizen. In that aim, most of industrial countries as USA and European countries have decided to establish the list of such services and to apply security measures to ensure their reliability. These services, which encompass energy distribution (electricity, gas, oil), emergency services, financial services, telecommunication, space services, have been called "critical" in a specific framework, the Critical Infrastructure Protection (CIP).

In the European Parliament resolution of 12 June 2012 on critical information infrastructure protection – achievements and next steps: towards global cyber-security, the European Parliament

- "*welcomes the Member States' implementation of the European Programme for CIIP*[1]*, including the setting-up of the Critical Infrastructure Warning Information Network (CIWIN)*, […]
- *acknowledges that the Commission is considering revising Council Directive 2008/114/EC and calls for evidence to be provided of the effectiveness and impact of the directive before further steps are taken,* […]
- *considers that ENISA*[2] *can play a key role at European level in the protection of critical information infrastructure by providing technical expertise to Member States and European Union institutions and bodies*".

Even if the text underlines the will of European parliament to support CIP, we interpret this text as a sign that the EU has limited authority to improve CIP. In respect of national sovereignty for security matters, they rather encourage this to be done at national level, as can be seen form recent publications:

1. In the setup of the Critical Infrastructure Warning Information Network (CIWIN), the EU aim is defined as follows: "with the help of *assisting* Member States to *exchange information on vulnerabilities* and appropriate measures and strategies to mitigate risks related to CIP". Originally, CIWIN intends to be an alerting system, but not only an information sharing system. This alerting has been postponed to a second phase.

2. In the proposal for a directive concerning measures to ensure a high common level of network and information security (NIS) across the Union: "This will be achieved

[1] CIIP = Critical Information Infrastructure Protection, is the ICT related part of CIP, dealing in particular with cybersecurity, e.g. attack from Internet.

[2] ENISA = European Union Agency for Network and Information Security, originally European Network and Information Security Agency, created in 2004 by EU Regulation No 460/2004.

by requiring the Member States to increase their preparedness and improve their cooperation with each other, and by requiring operators of critical infrastructures, such as energy, transport, and key providers of information society services (e-commerce platforms, social networks, etc), as well as public administrations to adopt appropriate steps to manage security risks and report serious incidents to the national competent authorities." (cf. COM(2013) 48 final of 7.2.2013).

However, as demonstrated by the Stuxnet malware, the complexity of such an attack exceeds any national level.

1.4 The challenges

Indeed, two lessons should be derived from recent attacks: first we need better care on security and risk management of Critical Infrastructure. Secondly, as prevention cannot be perfect, we should better monitor security aspect to detect and block cyber-attacks, or at least, to mitigate their impact on the entire systems.

Marc Elsberg's novel illustrates well the consequences of unwillingness by national regulator and private operators to alert or shared their information on risk with other entities.

To face these challenges, political decisions cannot provide quick solutions. The ball is in the court of security experts and CI operators to find relevant, smart and economic sustainable solutions to improve their security.

2 A specific response: the CockpitCI project

2.1 CockpitCI project genesis

In a previous research project, called MICIE; with a focus on electricity grids, we concluded that it is imperative to design systems which allow operators to assess the operational risks, to promptly communicate such risks with interested parties, so that they can prepare suitable containment and prompt risk treatment.

At the end of this project, itrust consulting together with most research partners of MICIE defined a new project proposal to apply lessons learned to Cybersecurity. This proposal was retained for funding by the EU Commission.

The European research project CockpitCI, acronym for "Cybersecurity on SCADA[3]: risk prediction, analysis and reaction tools for Critical Infrastructures" started in early 2012. With a total cost of 4,3 Mio € of which almost 3 Mio are funded by the EU, the project aims to create a framework and tools enabling the detection, analysis, and real-time information sharing of cyber-attacks in order to assess risks and avoid disastrous cascading effects.

2.2 itrust involvement in the project

Within CockpitCI, itrust consulting participates in the description and modelling of the cyber-attacks, modelling and prediction of Quality of Service, in the development of parts of the analysis tool, in the design of security requirements and operational requirements of the Secure Mediation System, and in trial and dissemination. itrust leads the dissemination by organizing workshops, hosting and feeding the website, organizing demonstrations for CI operators.

As preliminary results, itrust consulting has developed two detection probes of the CockpitCI tool, which can also be used as independent tools: AVCaesar and Software checker.

2.3 A meta-antivirus: AVCaesar

AVCaesar is a meta-antivirus that combines several antivirus programs that perform an in-depth scan of any file exchange between sensitive networks like SCADA and IT, and the corporate networks often linked to the internet. This tool can also be used by security incident analysis teams in order to scan and pre-analyse suspicious files.

AVCaesar can be used to:

- Perform an efficient malware analysis of suspicious files based on the results of a set of antivirus solutions, bundled together to reach the highest possible probability to detect potential malware;
- Search for malware samples in a progressively increasing malware repository managed by malware.lu CERT, a brand of itrust.
- Generate an incident report in a specific format (i.e. IDMEF format) to feed automatic analysis tools as in CockpitCI PIDS (Perimeter Intrusion Detection System).

The tool currently integrates antivirus tools like Avast, AVG, Avira, ClamAV, Emsisoft, ESET NOD32, GData, Kaspersky, McAfee, Microsoft Essential Security.

In future, AVCaesar can also be installed as software appliance in the security infrastructure of CI operators.

2.4 Vulnerability detection agent: software checker solution

After installation of a light software client on machines spread over the monitored network, Software Checker informs a server integrated in the CockpitCI tool, on the installed software, key elements of the configuration, and potential vulnerability of the software according to vulnerability databases like OSVDB. This is an essential input for assessing the risk level, but also a starting point for detecting installed malware.

The first version of Software checker verified whether Windows operating systems contains software with security vulnerabilities and warns whether updates of software are available. Future versions will allow managing this information centrally, collecting information from Unix system and even embedded system, and using it for predicting potential attack, and also for planning upgrading actions.

3 3rd CockpitCI Workshop on "SCADA Cybersecurity" in Luxembourg.

On March 10th 2014, itrust consulting and CREOS, under the patronage of Étienne Schneider, Minister of Economy and Foreign Trade, organised the 3rd CockpitCI Workshop on "SCADA Cybersecurity" at Creos' national dispatching centre.

This workshop enabled the European Agency for cyber security, Luxembourgish authorities (Ministry of Economy, GOVCERT.LU, HCPN), the national electricity and gas provider CREOS and other Luxembourgish industrial attendees as well as the project partners including the security consultancy and research company itrust consulting, the CRP Henri Tudor from Luxembourg, the project coordinator Selex ES from Italy, Romanian operators, and researchers from Italy, Portugal, Great Britain, Israel, Norway and Belgium to discuss the problems

[3] SCADA = Supervisory Control and Data Acquisition, means a type of industrial control system (ICS) often used for managing a Critical Infrastructure, e. g., the management of the electricity distribution system.

and solutions concerning the security of critical infrastructures.

As opening talk to the workshop, the authors of this article referred to new security standards in this domain like the IEC 62442 family and to the importance of communicating risks between CI professionals and being prepared in order to react effectively in case of an attack.

Mr François Thill of the Ministry of Economy assured the audience of the Ministry's support to all Luxembourgish initiatives focusing on acquiring the necessary competencies in order to protect the electricity, gas and water supply against malicious attacks.

Carlo Bartocci, responsible of Creos' dispatching, spoke about technical problems encountered during the migration of their current control management system. The improved performance of supervision systems makes them increasingly more complex and thus it is more difficult to find flaws, being it unintentional errors like simple technical incompatibilities or even worse intentional threats like a malware. His presentation highlighted why it is extremely important to protect SCADA networks from the open telecom network, why data flows should be traced, why functional and security tests before changing are mandatory, and when detailed monitoring is needed.

Adrian PAUNA, NIS expert at ENISA, presented several European initiatives: first, ERNCIP aimed at sharing knowledge to harmonise test protocols, second, the recommendations to use security certified products, and third, the recent project for cybersecurity skills certification of SCADA experts. He invited all experts to participate in their ICS SCADA Expert Group.

Paul Rhein, Haut-Commissariat à la Protection National (HCPN), presented Luxembourg's governmental actors in cybersecurity, like the CERTs, and their coordination bodies. A new law should increase the importance of cybersecurity and crisis preparedness, as a reaction to the fear expressed by the EU commissioner Neelie Kroes that "self-regulation does not work here".

In the second part of the workshop, Antonio Graziano from Selex ES, Italy, presented the CockpitCI project. He compared the new cyber threats on control systems with an F16 jet attacking a WW1 battlefield. The CockpitCI system under construction should be a decision making system in passive mode; detecting, analysing and managing cybersecurity risk in real time. Prof Paulo Simões, University of Coimbra (Portugal), explained a main part of the system, i.e. the detection architecture: In a distributed network, probes bring security information from IT networks, Operator networks, and Field networks to the Security Management Platform. These probes or detection agents are part of smart perimeter intrusion detection systems (PIDS), including HIDS, NIDS, fieldbus honeypots, software and configuration checkers, etc., and analysis tools such as correlators or OSVM engine (cf. figure). Prof. Stefano Panzieri, University of Roma Tre, illustrated the On-Line Risk Prediction System. He discussed interdependency models, knowledge bases with countermeasures, risk assessments, etc., to process the detected information. If needed, this system alerts and proposes counter-measures to the control centre through a so-called Cockpit. Prof. Michele Minichino from ENEA Italy illustrated the underlying models established in CockpitCI for an electrical grid, for the virus spreading over this grid, and for the Fault, Location, Isolation and Restoration system (FSIR) behaviour in case of virus attacks. Prof Leandros Malgaras from the University of Surrey (UK) presented a tool for the consolidation of detection information based on "One Class Support Vector Machines" (OCSVM).

Finally, itrust consulting demonstrated for the first time two tools it has developed under CockpitCI: AVCaesar and Software Checker.

In the after-workshop-discussion, the participants discussed the importance of developing complementary competencies which enable the detailed analysis of sophisticated cyber-attacks. itrust consulting, which is operating the first private CSIRT (Computer Incidence Response Team) in Luxembourg, called "malware.lu CERT", and which is in partnership with CIRCL and GOVCERT.LU is motivated to assist control system operators in this challenge.

4 Smart Grid Luxembourg – Cockpit (SGLC)

As a follow-up of CockpitCI, some national actors: itrust consulting, Luxmetering GIE, and CREOS, as well as the interdisciplinary Centre Security, reliability and Trust (SnT) of the University of Luxembourg, decided to launch a project to develop a real-time cyber risk monitoring tool, primarily dedicated to monitor the security of the future national smart grid. The project is co-funded by the Ministry of Economy and aims to finish in 2016 with a security monitoring tool acting passively on the smart-metering management system. As such it intends to provide an overview on security and operational risk, to be used by security management, independently of the manufacturer, the integrator, and the team of operators of the smart-metering managing system.

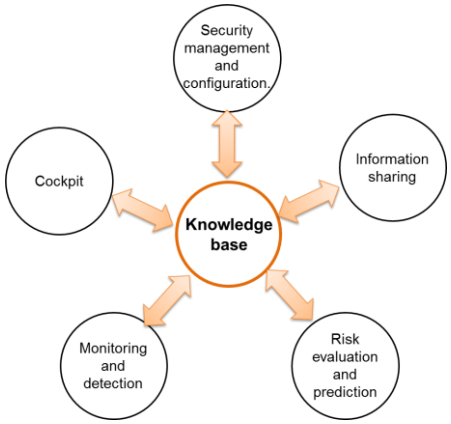
SGLS aims at modelling, developing and testing tools and techniques for monitoring cyber-security aspects of smart-meters in the context of the Luxembourg Smart Grid Project (SGL 2.0). These tools and techniques could then be used to manage and control the security of the smart meters that will be installed in the Luxembourgish grid. The use of these tools is not limited to smart grid. Indeed, they could be extended to address the need of other operators of critical infrastructure (e.g. water grid operator) which could also be the target of cyber attacks.

Moreover, the research collaboration aims at combining security risk analysis with real time indicators based on measures on the operational infrastructure. For this reason, the Cockpit SGL project consists in completing the existing basic security architecture by relying on a risk analysis approach, which will use real time indicators of the level of cyber security risks. In addition to this, a new security events detection system will be put in place, based on the deployment of an intrusion detection system that will monitor during real-time and raise alerts when potential attacks are detected. These two main components (the risk analysis element and the event detection element) will be located in the same central supervision and management system.

In particular, the project will focus on the hacking of smart meters under test in Luxembourg. This type of hacking could be the first vector attack to a deeper attack targeting vital systems located in smart grid system. In that aim, the project will perform:

- Analysis of malware targeting first smart meter and secondly systems and devices belonging to critical infrastructure network
- Modelling, research and implementing of detection mechanisms
- Adaptation of malware.lu CERT to the specificities of smart meters.

The logical functions of the supervision tool are illustrated in following figure:



Outlook

Protection of critical infrastructure has been recognised as a priority, at EU and national level. In a series of research projects including participation from Luxembourg, methods and technology for better protection are being developed. Several actors, thanks to EU and national funding, deal with developments of appropriate and better security than what is operated today.

Whether these security measures will be deployed depends on the society readiness to pay for security. Today's population has never lived a longer period without electricity, without gas, without telecommunication, without internet or banking services, or most important without food or automatic water provisioning. It has never lived other situations than peace and public control. This, however, is not a default situation; it needs protection; it has a price to pay for. Natural disasters, like the tsunami in Fukushima, have created in the past greater damages than deliberates attacks. Nevertheless, cybersecurity, research results, or recent tests, like stress test on nuclear power plant, demonstrate the feasibility of high damaging attacks, and the still insufficient protection against cyber-attack. Predicting such risk is difficult. For natural disaster we can use statistical evidence to estimate the probability of occurrence. For cyber-attacks, this is far more difficult, as there cannot be historic evidence.

Mutual trust and readiness to share knowledge is a prerequisite of effectively managing the next cyber-attacks. Insiders know that security has a price, not negligible, but far lower than the impact of attacks. They also know that past resources have been insufficient to counter serious attacks.

Pessimists claim that 100% security is not possible, and they often try to abuse this argument to justify an ineffective security or stagnation of today's countermeasures. But if 100% security is not possible, to decrease the impact of such risks by effective counter-measures is handy.

Critical Infrastructure Protection is mandated by social responsibility. Protection against cyber-attacks merits more public attention, to make sure that interested parties, in particular all citizen benefitting from our economically wealthy situation, are ready to invest resource in protecting them against all kind of malicious intentions.