A structural design for a pan-European early warning system for critical infrastructures

H. Kaufmann, R. Hutter, F. Skopik, M. Mantere

The protection of critical infrastructures increasingly demands solutions across interdependent infrastructures all over Europe supporting incident detection and management. This necessitates cooperation of privately owned infrastructure operators and public bodies between sectors and across borders. The ECOSSIAN project, funded by the EU under the 7th framework program for research and development, develops a prototype of such a holistic system based on use cases from the sectors energy, transportation, and finance. The system uses a multi-tiered architecture and incorporates advanced technologies, including fast data aggregation, situational visualization, planning and decision support, and flexible information sharing and coordination support networks. The technical solutions will be complemented by an organizational concept, corresponding rules and regulations, as well as factors of societal perception and appreciation. This positional paper gives an overview of the ECOSSIAN concept and architecture.

Keywords: pan-European critical infrastructure protection; cross-organizational security information sharing; early warning system; cyber incident management; architectural design

Ein Architektur-Entwurf für ein europaweites Frühwarnsystem für kritische Infrastrukturen.

Der Schutz kritischer Infrastrukturen verlangt zunehmend nach europaweiten Lösungen in allen zusammenhängenden Infrastrukturbereichen, welche das Erkennen und das Management von Störungen unterstützen. Dies erfordert die grenz- und sektorübergreifende Zusammenarbeit zwischen den in Privateigentum stehenden Infrastrukturbetreibern und den öffentlichen Einrichtungen. Das unter dem 7. Rahmenprogramm der EU für Forschung und Entwicklung geförderte Projekt ECOSSIAN (European Control System Security Incident Analysis Network) entwickelt derzeit einen Prototypen für ein derartiges holistisches System basierend auf Anwendungsfällen in den Bereichen Energie, Transportwesen und Finanz. Das System verwendet eine mehrstufige Architektur und umfasst die modernsten Technologien, inklusive schnelle Datenaggregation, Lagebildvisualisierung, Planung und Entscheidungsunterstützung sowie flexible Informationsaustausch- und koordinationsunterstützende Netzwerke.

Die technischen Lösungen werden darüber hinaus durch ein Organisationskonzept, entsprechende Richtlinien und Regelungen sowie andere Faktoren wie gesellschaftliche Wahrnehmung und Wertschätzung ergänzt. Dieser Beitrag bietet einen Überblick über das Konzept ECOSSIAN und dessen Architektur.

Schlüsselwörter: europaweiter Schutz kritischer Infrastrukturen; organisationsübergreifender Austausch von Sicherheitsinformationen; Frühwarnsysteme; Management von Cyber-Zwischenfällen; Architektur und Design

Received November 10, 2014, accepted November 24, 2014

1. Introduction

Modern society strongly depends on the continuous and reliable availability of a number of products and services. In the case of serious disruption, consequences for the society as a whole can be drastic. This holds especially true with the services provided by so called Critical Infrastructures (CI), such as energy, transportation, finance, and so on. Critical infrastructures are mainly comprised of diverse control systems. In the past these control systems were mostly isolated, independent and proprietary systems with no connection outside the control loop (air-gap). CIs are driven by the many challenges including being more economical, more flexible, more efficient and sufficiently reduce energy consumption. These challenges are answered by increased interconnections and utilization of advanced networking technologies. For economic reasons, these cyber-physical systems more and more rely on commercial-off-the-shelf (COTS) products. Thus the attack surface of control systems increases significantly by introducing threats and vulnerabilities into control systems, previously only found in enterprise networks.

Therefore it is crucial to get an overall situational picture, especially also considering interdependencies [2], which is necessary for a consistent reaction to security breaches and mitigate possible cascading effects. This is also true for the European Union as a whole, regarding the interdependencies throughout the Member States. A cornerstone for that is a real-time information sharing system and therefore an early warning system for cyber threats and incidents comparable to already established warning systems for physical threats and natural disasters. To address this issue the ECOSSIAN (European Control System Security Incident Analysis Network)

Kaufmann, Helmut, Airbus Group Innovations, 85521 Ottobrunn, Germany (E-mail: helmut.kaufmann@eads.net); **Hutter, Reinhard,** Centre for European Security Studies, Grünwalder Straße 155a, 81545 Munich, Germany (E-mail: hutter@cess-net.eu); **Skopik, Florian,** Austrian Institute of Technology, Donau-City-Straße 1, 1220 Vienna, Austria (E-mail: florian.skopik@ait.ac.at); **Mantere, Matti,** VTT, Radiomastontie 8 as. 6, 90230 Oulu, Finland (E-mail: matti.mantere@vtt.fi)

project[1] aims to develop an innovative structural design for a cross-sectoral and cross-border early warning system for critical infrastructures regarding cyber-security threats. The novelty of ECOSSIAN lies in the fact that in contrast to many others the topic 'cyber security information sharing' is not just dealt with in the technical dimensions, but holistically, including regulatory, legal and organizational aspects. This interdisciplinary approach is one of the key strength of ECOSSIAN.

2. The ECOSSIAN concept

Stuxnet proved that the currently applied security models and components such as firewalls, intrusion detection systems, anti-virus tools, "air-gap" and the like are not directly applicable and sufficient in control networks due to their special needs, including real-time issues, specialized protocols, resource constraints and interdependencies with other services. Therefore the view on security has to be reconsidered.

2.1 Overall concept

Our approach is based on distributed network and system monitoring where legacy systems, with limited or no monitoring and logging functionalities, are integrated as well. A cyber security monitoring and detection module will be implemented as a passive overlay network. This approach can be seen as an additional process safety component, because not only cyber-attacks can be detected in real time, also misbehavior and failure in the process control system can be recognized. This approach is able to detect and prevent an attack like a man-in-the-middle attack as conducted by Stuxnet. Yang Liu and Young Guan [6] propose to utilize a Network Operation Centre (NOC) to deal with this distributed data aggregation. The ECOSSIAN approach extends this proposed NOC to an Operator Security Operation Center (O-SOC), where operators have the ability to get a real-time view on the cyber security state of the control network and the processes controlled. The raw data behind this information will be stored and aggregated. The raw data can be used later on to conduct forensic analysis of incidents.

2.2 Critical infrastructure dependency model

However, securing each operator site in an isolated fashion is not enough. Because complex threats to interconnected infrastructures would frequently remain undetected. It is also obvious that the implementation of one O-SOC is not enough to protect a nation's sovereignty as a whole. Taking this into account it is necessary to establish an O-SOC in each sector and at each operator of critical services, and share information between them. Therefore the need for a trusted instance beyond each individual operator is given to share sensitive information between them and to enable a nation-wide situational awareness on the cyber security state of the national critical infrastructures. We addresses this issue by proposing the establishment of a National Security Operation Centre (N-SOC) for critical infrastructures. All O-SOCs of a nation are connected to the trusted N-SOC (see Fig. 1). Aggregated data on cyber-attacks and incidents will be shared between each O-SOC and the corresponding N-SOC of a Member State. To enable data sharing capabilities, we apply existing industry-standard data formats [8] with a possible extension to cover the ECOSSIAN requirements. This includes guaranteeing anonymity and privacy as well as confidentiality regarding an operator's infrastructure design and intellectual properties. The N-SOC approach will deal with high-level information from O-SOCs to determine a situational awareness and derive a cyber-security state view on a nation's critical infrastructure.

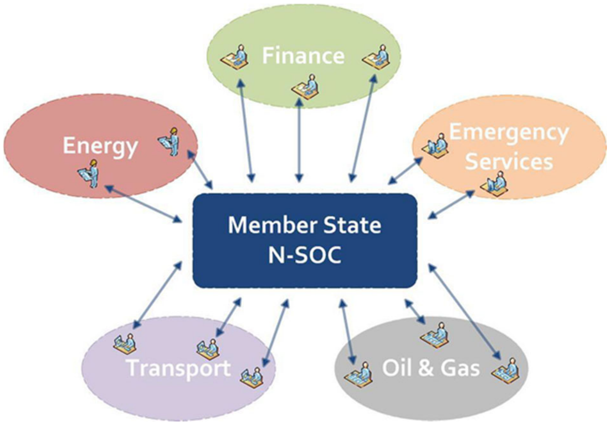


Fig. 1. N-SOC information sharing, early warning and incident response

The N-SOC models the interdependencies of a nation's critical infrastructure and provides the ability to share attack and incident information across stakeholders and to mine the information to analyze an attacker's intention and predict the probable spread of the attack to other critical infrastructures. Based on the detection, occurring threats can be mitigated or prevented by informing the individually affected operators through their interconnection from the N-SOC and the corresponding O-SOC. The view of CIs will be a *multi-layered* model which shows the various interdependencies concerning:

- Single infrastructure providers,
- Infrastructure sectors (usually covered by several providers),
- Cross-sector interrelations and interdependencies,
- Cross-national/EU-wide interrelations and interdependencies.

To address the interdependencies between the critical infrastructures of different member states, we propose a European CI Security Operation Centre (E-SOC) as a third tier in its early warning and incident response/management framework. The capabilities, which shall be provided by the E-SOC are similar to what the N-SOCs support. The member states' N-SOCs are interconnected via the E-SOC. We will implement the SOCs on all levels as virtualized operation centers. This approach is an advanced collaboration tool for cyber-defense. The capabilities to be developed are cooperative preparation of cyber-defense, enhanced situational awareness, decision support for cyber-defense and countering sophisticated attacks. These capabilities will be implemented in a virtual environment by representing virtual spaces and rooms and populated with avatars from each joining stakeholder.

In case of the need for a consistent European response on an orchestrated attack against European member states' critical infrastructures, the advantage of the virtual command & control feature of the E-SOC gets obvious. It can be used to manage such incidents and mitigate the impact for each member state and the European Union as a whole.

ECOSSIAN can also be considered as a critical infrastructure. Therefore the protection of ECOSSIAN has to be addressed because there are several serious threats that can arise. Adversary attacks can emerge from the technical domain, e.g., command and fraudulent information injection or abuse of the system through distributed denial of service attacks. We have to implement technical measures to avoid evading technical restrictions.

[1] EU FP7-SEC-2013-1, grant agreement 607577; web: http://www.ecossian.eu.

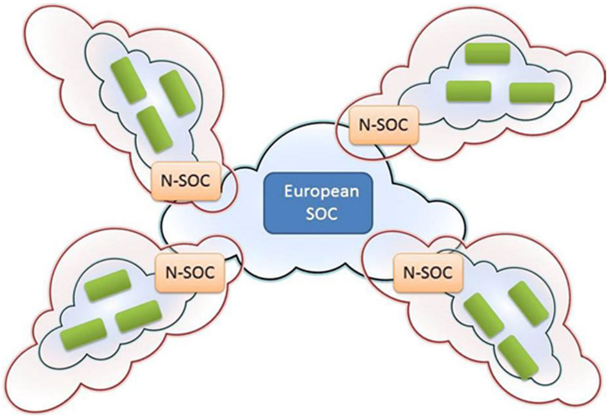


Fig. 2. The ECOSSIAN cloud

2.3 Secure virtual private community clouds

We address this challenge by defining and implementing Secure Virtual Private Community Clouds (S-VPCC). Each member state is based in its own S-VPCC comprised of the N-SOC and all national O-SOCs. The E-SOC resides in its own S-VPCC in conjunction with the member states' N-SOCSs (see Fig. 2). This means that only the N-SOCs are located in two S-VPCCs. Due to sensitive nature of information exchanged between SOCs within S-VPCCs we will use techniques such as pseudonymization or anonymization and enrollment policies.

The hierarchical three tier approach is:

- providing a European cross-country early-warning system,
- improving the understanding of cross-country (inter-)dependencies,
- improving the understanding of the cause of failures or attacks to the infrastructure, particularly when interdependences occur,
- enabling European-wide situational awareness,
- providing a central communication point for cross-border incident management.

3. Related work

Protection of critical infrastructures has been studied at the European level since about 12 years. Starting in DG INFSO with early studies on phenomena and possible roadmaps (e.g., DDSI, ACIP), projects in PASR[2] became more and more solution-oriented, followed by concrete work in the FP6 and FP7 security research area. Several documents, including directives, address protection of CI (e.g., EPCIP, CIWIN) and some communities are working on specific issues (e.g., TNCEIP[3] for the energy sector). ECOSSIAN will build on a number of results and experiences from past and current European projects (FP6/7, in the SEC and ICT themes) as well as national projects.

ECOSSIAN will be built on the results and approaches of these projects by developing a holistic, integrated and user friendly early warning system for all stakeholders from operators, member states and the European side while complying to legal and regulatory requirements.

The exchange of data and the sharing of information are commonly understood to improve the attack mitigation or resistance by combining forces. This is a prerequisite for situational awareness across borders. Consequently, secure and trusted communications, information exchange and suitable standards are often less a matter of technical solution but rather of cooperative openness as well as procedures and conventions (e.g., legal framework) to be agreed and established [9].

Generally, a central cross-border and cross-sector coordination in CI disaster or incident management does not exist or is at maximum rudimentary. The latter is true both in terms of technologies as well as in terms of agreements and procedures between sectors, and between governments and private sectors. At European level, procedural and organizational approaches are being started with directive 114 [1] and follow-on actions. Several technical implementations are being performed in the EPCIP[4] program, e.g., the critical infrastructure warning and information network CIWIN, and a joint European network of secure test centres for reliable CI—controlled critical energy infrastructures. Numerous further projects and studies have been launched, several of which will serve as starting points of or input for the ECOSSIAN project. They particularly include several projects on anti-terror preparedness and strategies for improving CI-interdependency effects in CI networks.[5] ECOSSIAN will foster to provide required technologies and support the needed operational processes. National programs will supported, e.g., the German program KRITIS.[6]

Standards bodies released a large amount of reports on how to establish security information sharing networks: the NIST guideline 'Framework for Improving Critical Infrastructure Cybersecurity' [7], the ENISA documents 'Good Practice Guide on Information Sharing' [3] and 'Cybersecurity cooperation: Defending the digital frontline' [4] (just to name two of the many available guidelines from ENISA), or the ISO/IEC standard 27010 'Information technology—Security techniques—Information security management for inter-sector and inter-organizational communications' [5]. While these are important works, these recommendations are not the complete picture and important pieces are still missing in terms of operational security, applicable implementations, and compatibility to established processes. Hence, there is the strong need for further research regarding these aspects—which, eventually, will be covered by ECOSSIAN.

4. Conclusions

The main outcome of the ECOSSIAN project is to improve the detection and management of highly sophisticated cyber security incidents and attacks against critical infrastructures by implementing a pan-European early warning and situational awareness framework with command & control facilities. The heart of a supporting infrastructure is a suitable model for information sharing. Here an important design decision is whether high frequency data about common security incidents should be exchanged (in this case just doable in a rather automatic fashion due to expected large volumes) or sharing of low frequency incident data on complex and exceptional events (which is barely doable in an automated fashion due to its inherent need for human intelligence) is the main application area of this platform. The first case requires a platform that is able to collect,

[2] Preparatory Action on Security Research.

[3] http://ec.europa.eu/energy/infrastructure/doc/20121114_tnceip_eupolicy_position_paper.pdf.

[4] http://europa.eu/legislation_summaries/justice_freedom_security/fight_against_terrorism/l33260_en.htm.

[5] http://www.dgpj.mj.pt/sections/planeamento/programas-financeiros-da6727/programaprevencao/2007/sections/planeamento/programas-financeiros-da6727/programa-prevencao/2007/overview-2006-2007/downloadFile/file/EPCIP_2006-2007.pdf?nocache=1216722837.94.

[6] http://www.bmi.bund.de/SharedDocs/Downloads/DE/Broschueren/2007/Kritis.html.

analyze, classify and correlate automatically produced data in near-real time; while the second case demands a platform that allows humans to exchange very security-sensitive data in a trusted environment with peers.

Eventually, the actual outcome of ECOSSIAN can further be broken down as follows:

- development of a layered system architecture for a pan-European early-warning and situational awareness system being suited for cross-country and cross-sectoral collaboration for critical infrastructure protection;
- specifications of the requirements and necessary interfaces (including data formats built on standards) for Cyber Defence Operation Centres on operator (O-SOC), national (N-SOC) and European (E-SOC) levels;
- provision of a secure information sharing and collaboration platform based on the concept of Secure Virtual Private Community Clouds, inherently integrated with the early-warning and situational awareness system, and compliant to legal and other regulatory requirements;
- development and adoption of technologies and processes for threat detection, data analysis, aggregation, correlation and visualization, as well as threat mitigation and incident management according to the requirement to the ECOSSIAN system;
- evaluation of the regulatory, social and economic boundary conditions for a pan-European detection and management of cyber incidents on critical infrastructures as well as the possibilities for influencing the adaptation of these aspects;
- full-scale demonstration of the integrated ECOSSIAN system on all levels (O-SOC, N-SOC, E-SOC).

Acknowledgements

This work was partly funded by the European Union FP7 project ECOSSIAN (607577).

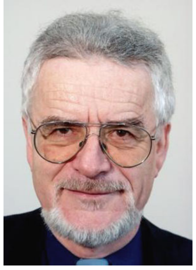
References

1. 2008/114/EC-Council Directive on the Identification and designation of European Critical Infrastructures and the assessment of the need to improve their protection, 2008.
2. Dudenhoeffer, D. D., Permann, M. R., Manic, M. (2006): Cims: a framework for infrastructure interdependency modeling and analysis. In Proceedings of the 38th conference on winter simulation. Winter Simulation Conference (pp. 478–485).
3. ENISA (2009): Good practice guide on information sharing.
4. Helmbrecht, U., Purser, S., Cooper, G., Ikonomou, D., Marinos, L., Ouzounis, E., Thorbruegge, M., Mitrakas, A., Capogrossi, S. (2013): ENISA: cybersecurity cooperation: defending the digital frontline.
5. ISO (2012): Iso/iec27010: information technology—security techniques—information security management for inter-sector and inter-organizational communications, 2012-03-20.
6. Liu, Y., Guan, Y. (2012): Distributed network and system monitoring for cyber-physical infrastructure. In Handbook on securing cyber-physical infrastructure. San Mateo: Morgan Kaufmann. Chap. 18.
7. NIST (2014): Framework for improving critical infrastructure cybersecurity, 2014-02-12.
8. Rutkowski, A., Kadobayashi, Y., Furey, I., Rajnovic, D., Martin, R., Takahashi, T., Schultz, C., Reid, G., Schudel, G., Hird, M., Adegbite, S. (2010): CYBEX: the cybersecurity information exchange framework (X.1500). In ACM SIGCOMM CCR.
9. Schoo, P., Schaefer, M., Egners, A., Hofinger, H., Wessel, S., Kuehnel, M., Todt, S., Montag, M. (2012): Collaboration between competing mobile network operators to improve CIIP. In Proceedings of the 7th international conference on critical infrastructure security (CRITIS).

Authors

Helmut Kaufmann

joined Airbus Group Innovations in March 2012 and is currently working in a transnational Cyber Operation Research Team with focus on cyber security in industrial control systems. Current research interests include applied research of secure collaboration, incident response, intrusion detection and honey technologies in SCADA environments. Before joining Airbus Group Innovations Helmut Kaufmann was professor for IT- and information security at the University of Applied Sciences St. Pölten, Austria. He has, so far, 20 years of experiences in cyber security earned as Safety and Security Manager at Frequentis AG which is an Austrian world market leader in secure flight control and air traffic management systems as well as a security consultant at the Raiffeisen Banking Group and as secure web specialist at the UNO at the preparatory commission for the comprehensive nuclear-test-ban treaty organization. He holds a master´s degree in Mathematics and Physics from the Vienna University of Technology, Austria, a masterś degree in Telematics Management from the Danube University Krems, Austria, and a degree in electrical engineering from the Technical College St. Pölten, Austria.

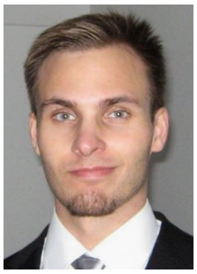


Reinhard Hutter

has a long standing log of technical and managerial skills and references, particularly in the field of security. He has done basic R&D in electronics and control systems at Siemens before he focused on Operations Research and Command Control and Communications at IABG. He has been manager of large scientific organisations and of major international projects. His management career went up to Senior Vice President Information and Communication Systems, and SVP European Security Analyses. Since 1995 he has concentrated on the evolving security challenges including cyber warfare, critical infrastructure protection and crisis and disaster management, and he has successfully acquired and managed numerous related national and EU projects with focus on advanced methodological approaches. He is a recognised expert, both nationally and in the international community in these domains. In 2006, Mr. Hutter was co-founder and is now technical director of CESS, the Centre for European Security Strategies, www.cess-net.eu/.

Florian Skopik
joined AIT in 2011 and is currently working in AIT's ICT Security Research Team as Senior Scientist, where he is responsible for national and international (EU FP7) research projects. The main topics of these projects are centered around smart grid security, the security of critical infrastructures and national cyber security.

Prior to joining AIT, Florian received a college degree in Electrical Engineering in 2001, as well as a bachelor degree in Technical Computer Science in 2006, and master degrees in Computer Science Management and Software Engineering and Internet Computing from the Vienna University of Technology, Austria, in 2007. He was with the Distributed Systems Group at the Vienna University of Technology as a research assistant and post-doctoral research scientist from 2007 to 2011, where he was involved in a number of academic research projects. In context of these projects, he also finished his Ph.D. studies and obtained a doctoral degree in Computer Science (2010) and a second doctoral degree in Social and Economic Sciences (2013). He published around 75 scientific conference papers and journal articles, and is member of various conference program committees and editorial boards. In parallel to his studies, he was working in the industry as firmware developer for microcontroller systems for more than 10 years. Florian is IEEE Senior Member and Member of the ACM.



Matti Mantere
received his M.Sc. in Information Engineering at the University of Oulu, Finland, in 2008 and is currently in the final stages of obtaining his D.Sc. with information security focus at the same university. He has worked as a Cyber Security Team Leader and later as a Senior Scientist at the VTT Technical Research Centre of Finland. He left VTT for another employment during August of 2014, but continues to work on information security for industry.