PREEMPTIVE

FP7 SECURITY 2013 - Grant Agreement No. 607093

Preventive Methodology And Tools To Protect Utilities

D4.4 PREEMPTIVE guidelines for improving Critical Infrastructures (CIs) surveillance

(01.03.2016 – 17.03.2017)

Deliverable Identifier:	D4.4
Delivery Date:	17.03.2017
Classification:	Public
Editor(s):	Federico Griscioli ENCS - UNIROMA3, Babatunde Kassim HWC
Document Version:	0.9
Contract Start Date:	March, 1^{st} 2014
Duration:	36 months
Project Coordinator:	Vitrociset S.p.A. (Italy)
Partners:	VITROCISET S.p.A., Universiteit of Twente, SecurityMatters BV, Aplicaciones en Informatica Avanzada S.L., Fraunhofer-Gesellschaft Zur Foerderung Der Angewandten Forschung E.V, HW Communications Limited, Universit degli Studi Roma Tre, European Network For Cyber Security Cooperatief Ua, The Israel Electric Corporation Limited, KU Leuven, Fundacio Institut De Recerca De L'energia De Catalunya, HARNSER Limited.

This project has received funding from the European Unions Seventh Framework Programme for research, technological development and demonstration under grant agreement No. 607093.

Document Control Page

Title	D4.4– PREEMPTIVE guidelines for improving Critical Infrastructures (CIs) surveillance	
Editors	**Name**	**Organization**
	Federico Griscioli ENCS - UNIROMA3, Babatunde Kassim HWC	
Contributors	**Name**	**Organization**
	Andrew Buick	HARNSER
	Elisa Costante	SM
	Jörg Kippe	IOSB
	Gladys León	AIA
	Regina Llopis Rivas	AIA
	Stephanie Mihail	KU Leuven
	Laurens Naudts	KU Leuven
	Steffen Pfrang	IOSB
	Maurizion Pizzonia	UNIROMA3
	Manel Sanmartí	IREC
	Antonio Ursini	VITRO
	Emmanuele Zambon	UT
Peer Reviewers	**Name**	**Organization**
	Laurens Naudts	KU Leuven
	Maurizion Pizzonia	UNIROMA
Format	Text – PDF	
Language	en-US	
Work-Package	WP4 - PREEMPTIVE Methodology Framework for utility networks	
Deliverable number	D4.4	
Due Date of Delivery	17.03.2017	
Actual Date of Delivery	17.03.2017	
Dissemination Level	Public	
Rights	PREEMPTIVE Consortium	
Audience	Public	
Date	March 17, 2017	
Revision	None	
Version	0.9	
Edited By	Federico Griscioli ENCS - UNIROMA3, Babatunde Kassim HWC	
Status	Project coordinator accepted	

Revision History

Version	Date	Description and comments	Edited by
0.1	Febrary 8, 2017	Preliminary table of contents v1	Babatunde Kassim
0.2	Febrary 17, 2017	Gathered lessons learned by PREEMPTIVE partners	Babatunde Kassim, Federico Griscioli
0.3	Febrary 28, 2017	Preliminary table of contents v2	Federico Griscioli
0.4	March 09, 2017	Added content	Babatunde Kassim, Federico Griscioli
0.5	March 10, 2017	Updated content	Federico Griscioli
0.6	March 14, 2017	Internal review	Maurizio Pizzonia
0.7	March 14, 2017	Updated Introduction according internal review	Babatunde Kassim
0.8	March 14, 2017	Updated sections according internal review	Federico Griscioli
0.9	March 16, 2017	Updated sections according LAurens' review	Federico Griscioli

Contents

List of Figures

List of acronyms - Definition

Acronym	Definition
APT	Advanced Persistent Threats
CI	Critical Infrastructure
SCADA	Supervisory Control and Data Acquisition
DSP	Distribution System Operator
ESCO	Energy Service Company
IDS	Intrusion Detection System
IDPS	Intrusion and Prevention System
NIDS	Network-based Intrusion Detection System
HIDS	Host-based Intrusion Detection System
IT	Information Technology
OT	Operational Technology
ICT	Information and Communication Technology
EC	European Commission
CII	Commercial, Industrial and Institutional
IoT	Internet of Things
PLC	Programmable Logic Controller
RTU	Remote Terminal Unit
DCS	Distributed Control System
EMS	Energy Management System
CIP	Critical Infrastructures Protection
NOS	Normal Operation State
USB	Universal Series Bus
OT	Operational Technology

Executive Summary

The PREEMPTIVE (PREventivE Methodology and Tools to protect utilitIEs) FP7 European Project aims at increasing the cyber-security of critical infrastructure and more specifically of Industrial Control Systems (ICSes). The main objective of the project was the developed of innovative detection and prevention tools that can be used to improve the cyber-security of different aspects of an ICS.

The main purpose of this white paper is to share the experience matured during the lifetime of the PREEMPTIVE project with people not involved in it, like critical infrastructure operators, regulators, and vendors. In this document, we share information that is not strictly related with the development of the PREEMPTIVE tools, but that stems from interaction and discussion within the project partners and with other experts. Based on our experience, we provide recommendations, and ideas for future works, which aim to help people ranging from technician to managers involved in the protection of utilities to improve their understanding of the complex problems they have to face at all levels. We deal with the major issues regarding the security of ICSes not limiting to the technical perspective but also covering aspects like management, legal compliance, and policies making.

1 Introduction

A critical infrastructure (CI) is defined as a system, a system of systems, and an asset either physical or logical, which is very valuable to a nation or organization and therefore requires protection [11]. Its operation is mostly monitored and controlled by industrial control system (ICS) such as supervisory control and data acquisition (SCADA) systems [8].

The initial design of the ICS was based on the isolation from the enterprise network since most of its operation was conducted locally. The remote location operation of ICS has grown rapidly over the last two decades with the integration of Information and Communication Technology (ICT) into the existing infrastructure through enterprise network.

Electricity, energy, gas, transportation, and complex distribution utilities rely on the availability of ICT infrastructures for the information exchange between different devices on the utilities of the control system [3]. SCADA networks are now able to utilize the existing telecommunication network infrastructures for accessing their network through the use of the remote access to configure and monitor field devices. Also many distributed controlled field devices such as Programming Logic Controllers (PLCs) and Remote Terminal Units (RTUs) are moving from a serial to an IP Ethernet base for their communication with the control center [5]. Most asset owners have embraced an IP based data exchange over the circuit switched approach, which has improved their day-to-day operations. The industrial control system consists at least of the following components:

- Supervisory Control And Data Acquisition (SCADA)
- Distributed Control Systems (DCS)

However, the integration of ICT infrastructure and IP Ethernet based communication used by PLCs and RTUs has exposed the ICS, and critical infrastructurse as a whole to different cyber-attacks in recent years. These challenges have prompted the need for enhancing the cybersecurity protection for ICS.

In this deliverable, we present the overall lesson learnt during the PREEMPTIVE project execution. We describe some of the cybersecurity challenges faced by critical infrastructure owners and provide technical and non-technical recommendations based on our experiences

and understanding gained throughout the PREEMPTIVE project.

This white paper is organized as follows: Section 2 describes some of the cyber-security challenges faced by existing utility provider of industrial control system that arise from integration of ICT infrastructures. Section 3 an overview of the PREEMPTIVE project. Section 4 a list of recommendation for the utility provider and critical infrastructure owner based on lesson learned during the project. Section 5 presents a future research work. The white paper is then closed with Section 6 that draws the conclusion.

2 Cyber-Security Challenges in Industrial Control Systems

The critical infrastructure is an embodiment of complex devices such as industrial control systems. CI operations have grown with the help of different commercial off the shelf COTS devices. The supervisory control and data acquisition (SCADA) system is an integral part of the critical infrastructure which is computer based industrial control systems, has scaled up its infrastructure to have little similarity to that of standard ICT infrastructure [7].As a result of this, vulnerabilities have been introduced to SCADA systems and the entire industrial control system which lead to most cyber-attacks incidents reported on critical infrastructures [15], [16].

The persistence attacks on industrial control system have drawn the attention of the utility owner to seek need for the cybersecurity protection of their utilities against cyber-attack. Many of the attacks are launched based on the knowledge gathered about the IT infrastructure in the ICS. While a traditional antivirus can provide protection against known threats, it cannot be solely relied upon against unknown and zero-day attacks. Some of the potential ICS threats are listed below:

- Insider Sabotage
- Advanced Persistent Threats (APTs)
- Coordinated cyber-physical attacks via remote or fixed connection
- Human Error due to inadequate training or carelessness
- Distributed Denial of Service (DDoS)

All these threats has impacted the cost of running operation of the industrial control system and critical infrastructure as whole. It is much more expensive to replace a system than to detect a cyber-attack on such a system, not only does it take time and money to install this system, the reputation of the utility owner is also often affected. The entire industrial control system is faced with not just cyber threats from the external but also the internal. There are more threats actors with the intention and capability to cause cyber-physical harm to the

industrial control system. Their motivation ranges from stealing critical information about the control system, causing catastrophic damage from cyber-attack to long-term espionage. Some of the recent attacks on industrial control system are listed below:

- Cyber-attack on German ICS iron plant in 2014 which cause breakdown in normal operation of the plant[4].
- An insider attack such as disgruntled employee sabotage the industrial control system of the waste water processing facility which causes spilling of the untreated waste water [19].
- An unauthorised backdoor access to the industrial control system created by disgruntled employee [22]

In order to overcome the cybersecurity challenges against critical infrastructure, it is imperative to look at new approach to protect the industrial control system within the critical infrastructure. The need for the cyber security surveillance and protection of the critical infrastructures is an important aspect of all critical infrastructures protection (CIP) plans. They should provide a guide for security managers/operators for improving the cyber security awareness and protection of their infrastructure. The PREEMPTIVE project is aimed at providing an industrial control system with innovative cybersecurity protection and a methodological framework for assessing cyber risks[1]

3 Preemptive Project at a Glance

The PREEMPTIVE (PREventivE Methodology and Tools to protect utilitIEs) FP7 European Project aims at increasing the cyber-security of critical infrastructure and more specifically of Industrial Control Systems (ICSes). PREEMPTIVE has built innovative detection and prevention tools and methodologies to face advanced attacks.

The key innovation of PREEMPTIVE is to combine the detection capabilities of multiple tools. Each tool can be integrated into different levels of the system and, are singularly able to detect a specific set of anomalies. By properly integrating the individual capabilities of each tool, the PREEMPTIVE framework is an effective defense against cyber-attacks using inventive approaches (e.g., APTs).

The architecture of PREEMPTIVE framework, depicted in Figure 3.1 is composed by IDSs, a correlation engine, and a graphical interface. A small description of the tools follows. For further details we refer to the project documentations published on the official website [1].
Host level IDSs [23]:

- IT-HIDS (Host-based IDS for IT components) monitors, audits, and detects potentials attacks against IT components used in ICS environment (e.g., SCADA servers, historian server, engineering workstations). It captures information about processes and programs activities in the host system in real-time in order to check potential threat patterns.

- ED-HIDS (Host IDS for Embedded Devices) monitors and checks anomalies in embedded devices used in ICSs in all different domains, such as for instance PLCs, Remote Terminal Units (RTUs), and Inteligent Electronic Devices (IEDs). ED-HIDS aims at detecting attacks with the intention of hijacking the control flow of a process and exploiting memory corruption vulnerabilities in order to execute arbitrary code.

- HIS (Host-based Integrity System) aims at guaranteeing integrity of storage devices (e.g., USB thumb drives). The purpose is to prevent the use of a USB thumb drive as a spreading vector of malwares. HIS allows the use of the USB memory stick both in critical system, namely, systems belonging to ICS that has to be protected, and in not critical system (general workstation, comprising personal ones) while preserving the security in term of integrity.

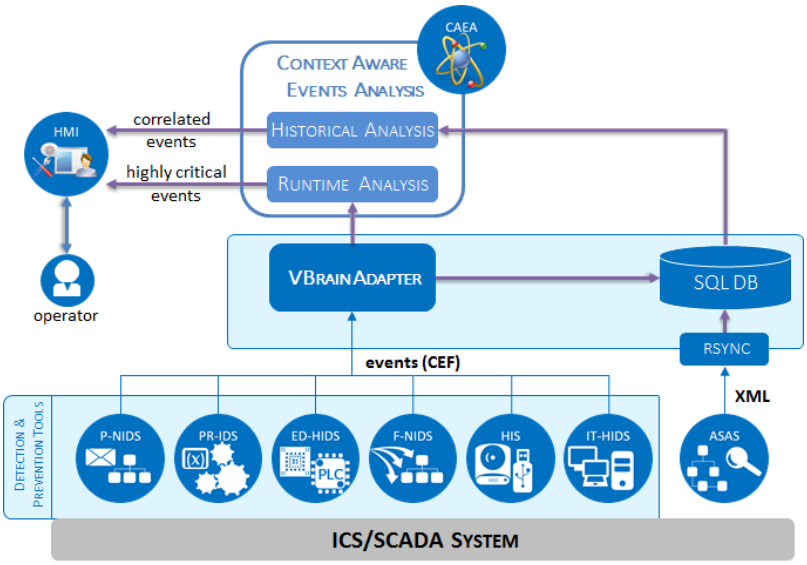

Figure 3.1: Architecture of the PREEMPTIVE framework.

- USBCheckIn is an hardware-solution able to protect any kind of USB host against BadUSB attacks [17]. BadUSB are attack techniques based on a modification of the device firmware, that forces the infected device (e.g., USB pen drive, USB ethernet card) to behave as a different kind of device, for instance a human interface device (e.g., mouse or keyboard). The basic idea of USBCheckIn is to authenticate the real USB human interface forcing the user to physically interact with it. USBCheckIn is compatible with every kind of devices which have an USB interface (e.g., embedded systems), hence, deployable within industrial control systems.

Network level IDSs:

- P-NIDS [6] (Payload-based Network IDS) aims at detecting semantic attack to ICSs by analyzing the content of the payload of network packets. It monitors process variables, learn their trend, and detects deviation from the normal behavior.
- F-NIDS [6] (Flow-based Network IDS) is a flow-based detection system. It monitors the traffic in the control network, namely, where the interactions between the supervisory system (SCADA) and the field devices (e.g., PLCs, RTUs, ...) take place. It characterizes the network flows to define a baseline which describes the normal behavior of the system. The detection of potential attacks is performed by identifying

deviations from such baseline.

- ASAS (ASset ASsessment) [13] is a vulnerability assessment tool that scans the network to discover the existing devices and provides hosts and network information (e.g., IP address, Operating System (OS), software version, open ports) in order to generate a network model and perform vulnerability scanning.

Process level IDSs:

- PR-IDS [14], [18] (Process Related IDS) is an anomaly-based detection system built using a multi-agent approach. It analyzes data at the industrial process level taking as an input, real-time data directly from the SCADA server. The first step is to transform the physical quantities measured into the Normal Operation State (NOS) by means data analysis methods. NOS defines the normal behavior of the industrial process and it is used for training and operation. Indeed, the detection phase aims at detecting any abnormal behavior which does not belong to the NOC.

Correlation engine:

- CAEA [18], [21] (Context Aware Event Analysis) is in charge of gathering all events raised by PREEMPTIVE tools, correlating, and analyzing them. When a tool detects a misbehavior, it sends a message with a well-defined set of information about the event to a *VBrain Adapter* that represents the interface with the correlation engine. The main purpose of the correlation engine is to correlate alarms sent by the tools in order to find relations that a first sight could seem unrelated but, instead, represent an unknown attack which could be undetectable by a single IDS.

PREEMPTIVE project provides also a methodology [12] that follows a *top-down* approach (described in Figure 3.2) and includes the following steps:

- Risk assessment methodology
- Asset identification
- Threat characterization
- Vulnerability assessment
- Technical guidelines

The output of the methodology is a collections of best practices representing the countermeasures to be applied to improve the level of security of the system on which the PREEMPTIVE methodology is performed.

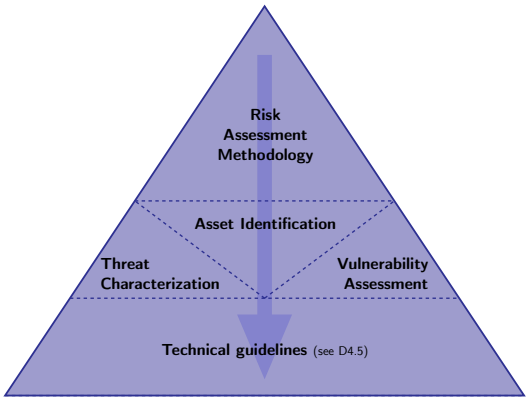

Figure 3.2: Approach of PREEMPTIVE methodology

4 Recommendations for Industrial Control System Security

In this section, we present recommendation guidelines that will help the cyber-security managers of the utility network on how to improve their critical infrastructure. The cyber-security managers includes the IT technicians and IT administrators. We do not intend to provide an exhaustive list of best-practices to enhance the security of this kind of systems. Our purpose is to share the experience we have matured during the lifetime of PREEMPTIVE project. In Section 4.1 we present a list of technical recommendations, in Section 4.2 we list non-technical recommendations that impact stakeholders potentially involved in the security of utilities.

4.1 Technical Recommendations

The following list is devised with the intent to inspire security experts and utilities managers of all different domains (i.e., gas, water, and electricity).

Cyber risk and economic impact. There is still a lack of knowledge, experience and understanding on the potential risks and impacts of cyber-security in the electrical distribution networks, especially in the deployment of smart grids technologies and, in general, in all utility domains. Cyber-attacks may damage equipment and have a significant economic impact for Distribution System Operator (DSO), retailer, Energy Service Companies (ESCO) and/or end-user.

Use of detection and prevention tools at different system level. No silver-bullet solution exists that (alone) can guarantee the security of critical systems. In general every solution comes with pros and cons and it can effectively protect, the target system only against a predefined set of cyber-attacks. Therefore, to increase protection it is necessary to apply a suite of integrated security solutions that act at different levels (e.g., host, network, process) within the critical systems.

Gather information from heterogeneous sources. It is very difficult to protect a utility against certain threats For instance, consider threats that leverage insiders with in-depth knowledge of the control process and with granted access to the system. A

higher level of protection can be achieved by collecting and correlating of information coming from different sources (e.g., physical access logs, camera logs, security events, network activities), as the pointed out by PREEMPTIVE [21]

Management of intrusion detection system complexity. The adoption of intrusion detection and prevention systems (IDPSs) placed at different levels of ICS is an effective way of monitoring and protecting the ICS components. On the one hand, this approach increase the chance to detect innovative and unknown attacks, but on the other hand, it introduces more complexity into the ICS. A properly management of the events raised by the IDPSs become essential for an evident effectiveness of the protection.

Security information event management. Security information event management (SIEM) collects, normalizes, and processes heterogeneous data from multiple devices. It can help security operators to overcome challenges of thousands of logs and alerts raised from different security devices spread across the SCADA network. Furthermore, SIEM provides an overview of the entire system, could decrease the false positives rate, and increases the capability to detect attacks correlating events which singularly could not be considered critical.

Process-level detection. Tools aimed to detect intruders at the process level should work ideally with process-data from the control-centre as well as from the field or the communication network. Data should be collected as close as possible to the measuring devices in order to increase chances such data have not been intercepted and changed by an attacker. However, utilities fear that having multiple agents getting data at different layers can increase the vulnerability of the CI. Then, it is important to design process-related detection systems to make sure these connections to different data sources do not affect the security of the system and/or make the network more vulnerable to attacks.

Historical process-level data. A common approach of intrusion detection tools is to have a starting phase of training in which they take as a input a normal operation historical data. The purpose of this stage is to instruct intrusion system to characterize a baseline which defines the behavior of the system when it is not under attack. During the PREEMPTIVE project we learned by experience that utilities usually do not tag anomalies in their historical data and thus they cannot always be sure to provide clean data recorded during normal operation. Therefore, domain expert knowledge becomes essential during training phases. Our suggestion is that utilities should work in this subject in order to be able to provide clean and useful historical data which will help to build more efficient detection systems and increase their security.

False positives rate. False positives rate could be a problem for IDS, especially, for those adopting anomaly detection techniques. Indeed, an high rate of false positives can be exploited by a potential attacker to circumvent system defenses overloading security personnel. For IDSs aiming to be effective becomes vital to decrease as much as possible the false positives rate in order to increase the benefit in term of security.

Self-configurable solutions. Existing solutions that apply process monitoring to discover attacks that undermine the correct functioning of a utility, typically relay on the availability of properly skilled operators to fine-tune the solution (e.g., a selection of the most critical process variables). Such solutions do not account for the fact that utilities operators are overwhelmed with activities related to the operation of the control system and rarely see security as a real issue. It is therefore necessary to create security solution that are as self-configurable as possible and that can immediately show their benefit e.g., by automatically catch the process semantic and critical variables.

Security by design. It is important that utilities push vendors of process control equipment to improve the security of their products. Part of this improvement consist of correcting the problems in the implementation of the standard security mechanisms implemented in real-time operating systems.

Encryption only when strictly needed. There is a recent trend towards the adoption, by standardization committee and industrial control system vendors, of end-to-end encryption technologies (e.g., TLS/SSL) in industrial network protocols, with the intent of improving security. We argue that, while the authentication and integrity features would be certainly beneficial, the complete encryption of the traffic would hinder the visibility of the network traffic by security tools such as intrusion detection systems capable of deep packet inspection, while not providing substantial security benefits. We believe that technologies providing authentication and message integrity would be sufficient in many application scenarios related to critical infrastructures.

4.2 Non-Technical Recommendations

The non-technical recommendations for industrial control system are related to some of the security challenges described in Section 2. The goal of this section is to provide guidelines to stakeholders who have critical issues regarding the protection of their industrial facility and incident managers.

Integrity Vs. Confidentiality. In order to ensure a sufficient level of cyber-security protection, it is crucial that the integrity and authenticity of data are enforced. At the same

tim, confidentiality should be also be ensured. Nevertheless, it seems that, among industry and legal experts, there is a focus on implementing encryption technologies as a means to improve cyber-security. For instance, privacy-by-design strategies put forward encryption as a key privacy and security protection mechanism. Encryption technologies might increase data confidentiality, but they may not always work towards achieving the required level of authenticity and integrity verification. Moreover, they could hinder the visibility of the network traffic by security tools. Therefore, it is important consider the effects of encryption on cyber-security and foster collaboration between industry and privacy experts in order to achieve a better balance between effective intrusion detection, security and privacy goals.

Incident reporting. The European Commission (EC) should encourage Member States and all relevant stakeholders to coordinate incident reporting and sharing of relevant incident related information. This should include information concerning attack patterns and other contextual data. This will help operators and relevant stakeholders to act effectively to protect system operations and develop effective countermeasures. The involvement of security software developers would be beneficial. If the latter are also kept up to date, tools might be better adapted to current risks.

Harmonization of legal requirements. The EC should facilitate agreements between Member States regarding a minimum level of harmonization on security and resiliency requirements and standards. This should establish the basis for national regulatory authorities to effectively measure security and assess the current state of the overall system security. This will also enable effective assessment and comparison of solutions provided by different organizations. In order to increase national, international and cross-border security, governments must support information sharing across countries, sectors and within the industry, and they must improve international cooperation on cyber security frameworks. In turn, industry operators would be provided a larger toolset in mitigating cyber-threats posed to their infrastructures. In addition, considering critical infrastructures importance and the potential wide-spread nature of the societal risks related to cyber-security threats, the legal framework should focus on all stakeholders in the cyber-security value chain, including the developers of security tools

Involvement of legal stakeholders. Due to the technical nature of cyber-security processes, legal research can be difficult because of the language gap that exists between technically and legally schooled individuals. This could in part be mitigated by making the legal environment more aware of required technical protection mechanisms, or technical functionalities, and vice versa. For instance, data protection legislation

requires information concerning technical activities to be provided in plain and easily understandable language. Dialogue should therefore be increased between all partners involved in order to ensure an adequate understanding of cyber-security difficulties. In addition, in the context of cyber-security tool development, it is difficult to pinpoint exact legal obligations, whether soft law or not, that can help in the development of cyber-security products.

Rise awareness and engage end-users. Though, in general, the dangers, scope and effects of cyber-security attacks have become well known, technology and similarly cyber threats continues to advance. Therefore, cyber-security knowledge among end-users should be continuously promoted. Market operators should be regularly educated, on a compulsory basis, concerning the changes to the critical infrastructures system related to cyber-security. Further, in-depth knowledge concerning cyber-attacks among security personnel and upper-higher management is required, as they are often in charge or responsible for undertakings investments in cyber-security tools. They are still often unaware of cyber-security risks or do not properly take into account the potential scope these might have. For instance, they might not be aware of the dangers of running old software packages and OS. In addition, if certain security activities are outsourced, it must be ensured that no vulnerabilities exist via these parties. Furthermore, even if the critical infrastructure systems are technically secure, damage and financial loss can also be incurred through social engineering attacks and similar manipulation. Contrasting these types of targeted attacks however requires pervasive awareness and training of all the personnel.

Information Sharing. The standardization and facilitation of information sharing should be made a priority. This should also include other Commercial, Industrial and Institutional (CII) sectors across Member States. This must include ICS-SCADA operators and incident handlers in standardizing information sharing concerning both best practices and also known threats across critical sectors.

National Risk Assessment. Governments should conduct risk assessments from a national perspective, with the aim to identify and assess risks and impacts for a nations general population, by adopting an open, transparent, and collaborative approach, involving all relevant stakeholders and taking into account the components of risk assessment processes, such as the PREEMPTIVE risk assessment.

Alignment of business needs and security requirements. One procedural issue related to the improvement of security features in real-time operating systems and embedded device firmware is the fact that, even if security updates are made available to utilities,

they may not be deployed in production environments. This is due to the fact that security is not yet regarded "important" enough to justify the extra work and possible downtime caused by the rollout of these security updates. We believe that this situation should be improved in the future, by better aligning the business needs with the security requirements inside utilities.

Communication between IT and OT department. We argue there is a lack of communication between the IT and OT departments which makes it difficult to implement detection tools at the process level. Basically because cyber-attacks targeting ICS frequently begin at the network level and the consequences travel all the way down to the process level where field components are located. Since IT departments know the network, they would be the responsible team for any cyber-security tool, however, the OT department has the expert knowledge about the process. Therefore, this is the most appropriate department to support the implementation of a process-level detection system. Consequently, there is a clear need for more coordination among IT and OT departments in order to drive the development of cyber-security process-related detection tools.

Improved knowledge of infrastructure. In order to provide better security protection it is recommended that both the cyber-security manager and IT operator of the utility network provider have enough knowledge of the critical cyber-infrastructures and physical components used within their domain. It could be also important limiting the outsourcing of the management of the network infrastructure in order to directly oversee the application of the security requirements.

Management lesson. From the management viewpoint we learned that serious edge technology proposals can be brought to life through sound research and testing in the boundaries of convergence of fields. The interdisciplinary work brings the beauty of dissent and the growth in knowledge domain. On the other hand from our strategic perspective we see potential future partnering in bilateral agreements, as well as possible overcoming the limitations last mentioned above by pursuing the opportunity to bring some of our existing IP and patents for OT in the utilities as complementary domain expert knowledge.

5 Future Research

This section provides different future research work that can leverage on the PREEMPTIVE project to further boost the industrial control systems security incident reporting and awareness within the critical infrastructures.

5.1 Cyber Security framework for IoT and industrial control system automation

The PREEMPTIVE project covers some aspect of major critical infrastructures environment which are electricity, water and gas with the focus on improving the cybersecurity incident reporting and awareness. It also provides a cybersecurity-framework which can be used to provide countermeasures against cyber attacks, comprising the more advanced. As for future work, the integration of internet of a things (IoT) for industrial automation is gaining awareness in use within the existing critical infrastructure. The cybersecurity experts and industrial control system operators should pay attention at providing a common cybersecurity framework for this integration. A possible work could oriented to provide a concrete and robust cybersecurity risk-based framework which looks at the vulnerabilities and the ripple risks due to the deployment of an IoT infrastructure. In order to conduct a better research in this area, the experts of the technical processes within the industrial control system has to learn and understand the IT infrastructure

5.2 Data mining for Data correlation

The deployment of security information and event management system within industrial control system environment could be a valid approach to simplify the security alerts management. If correlation, on one hand, increases the capability to detect cyber-attacks, on the other hands, introduces complexity 4.1. Indeed, SIEM could require hard-tuning to define effective events correlation rules. The adoption of data mining algorithms can help to improve the extraction of patterns or model from the collected data to be used for the creation of such rules. Forthermore, future works could be performed to limit the dependency of human interaction adopting machine learning techniques.

5.3 Detection system for process-level

The experience gained during the PREEMPTIVE project is that there is a clear need for more research, development and implementation of detection systems at the process level. There exists a wide variety of detection systems at network level, in part inherited from internet cyber-security systems, but little has been done in applying detection algorithms directly to the supervised process (field measurements). Currently, there exist only two commercial tools (Thetaray [20], and ICS2 On-Guard system [10]) that claim to work with measurement variables from the process level, but not much information about their detailed operation is publicly available. None of the utilities that we have interviewed during the project perform any type of detection at the process (physical) level.

5.4 Innovative techniques for encrypted-data detection

In the context of industrial control system could be needed the adoption of encryption to fulfill specific confidentiality requirements due to privacy concerns. The common methods adopted by network-based intrusion detection system, for instance, are not able to perform detection of encrypted traffic, they need to see the packets exchanged on the network in clear. It is worth investigating method like searchable [2] and homomorphic encryption [9] that enables data analysis for attack detection and data validity checks on encrypted data.

6 Conclusions

In recent years, we have been observing a growth of high profile cyber-attacks against industrial control systems. In the past the common approach was to isolate ICS (OT network) from the corporate network. The adoption of isolation approach made possible to limit efforts about cyber-security in ICSes. The results are systems which often use legacy software devised without any security perspective and with strict uptime requirements so that regular patching, update or migration to new solutions is unfeasible. Furthermore, the recent trend toward the integration of Internet connectivity in industrial environments has been introducing flexibility and usability, for instance controlling remotely the industrial process, but on the other hands, increased potentially vulnerabilities which can be leveraged by an attacker to take control of the system.

According to this scenario and considering the attacks are more and more skilled than the past, the common defenses result totally ineffective and pointed out the need of inventive solutions able to reduce chances that such attack (e.g., APT) succeed.

We deem the PREEMPTIVE project as a step-forward on the industrial control system defense. The integrated detection and prevention tools, the methodology, and the method of correlating security events increase considerably the capability to detect cyber-attacks, also the more advanced.

In this white paper, based by the experience evolved from the project, we presented technical and non-technical recommendations which can be a meaningful equipments for security technicians and managers employed in utilities.

We touched upon the main aspects concerning the security of industrial control system providing the main guidelines to be followed. We took into account both legal and technical aspects, that sometimes could result conflicting. For instance, the guarantee of data confidentiality has to be balanced with the adoption of intrusion detection systems due to the difficult of performing detection on encrypted packets. We also considered management problems, especially those regarding the importance of communications among different departments of the same company and external organizations. Finally, we presented possible future works that can inspire further research activities.

Bibliography

[1] PREEMPTIVE - Preventive Methodology and Tools to Protect Utilities. http://preemptive.eu, Mar 2014.

[2] C. Bösch, P. Hartel, W. Jonker, and A. Peter. A survey of provably secure searchable encryption. *ACM Computing Surveys (CSUR)*, 47(2):18, 2015.

[3] Bundesamt fur Sicherheit in der Informationstechnik (BSI). Analysis of critcal infrastructures: The acis methodology. Technical report, 2004.

[4] Bundesamt fur Sicherheit in der Informationstechnik (BSI). Cyberattack on a german iron plant, bonn, germany. Technical report, 2014.

[5] Centre for the Protection of National Infrastructure(CPNI). SECURING THE MOVE TO IP-BASED SCADA/PLC NETWORKS. Technical report, November 2011.

[6] E. Costante, F. Griscioli, B. Kassim, D. Lund, M. Pizzonia, and E. Zambon. D7.4 – Network-based tools. Technical report, PREEMPTIVE, 2016.

[7] European Union Agency for Network and Information Security (ENISA) . Critical Infrastructures and Services. Technical report, November 2016.

[8] FireEye. Industrial Control Systems and Critical Infrastructure. Protect Industrial Networks and ICS/SCADA systems from sabotage and espionage. Technical report, 2017.

[9] C. Fontaine and F. Galand. A survey of homomorphic encryption for nonspecialists. *EURASIP Journal on Information Security*, 2007(1):1–10, 2007.

[10] ICS@. On-Guard system. Based on a machine-learning system designed to learn industrial processes. http://ics2.com/, 2017.

[11] ISO/IEC. Information technology – Security techniques –Information security risk managment: ISO/IEC 27005:2011(E). Technical report, 2011.

[12] J. Kippe, D. Meier, S. Pfrang, X. C. Fons, G. E. Leon, M. Wrightson, T. Kassim, M. Pizzonia, F. Griscioli, E. Zambon, E. E. Miciolino, and A. Ursini. D4.2 – PREEMPTIVE methodology reference. Technical report, PREEMPTIVE, 2016.

[13] J. Kippe, F. Steffen Pfrang, and X. Clotet. D4.5 – PREEMPTIVE Methodology supporting tools reference. Technical report, PREEMPTIVE, 2017.

[14] G. Len, X. Clotet, G. Len, E. Constante, M. Pizzonia, and F. Griscioli. D6.2 – Multi-Agent Architecture. Technical report, PREEMPTIVE, 2015.

[15] National Institute of Standards and Technology (NIST). Guide to Industrial Control Systems (ICS) Security. 2013.

[16] National Institute of Standards and Technology (NIST). Framework for Improving Critical Infrastructure Cybersecurity. 2014.

[17] K. Nohl and J. Lell. Badusb–on accessories that turn evil. *Black Hat USA*, 2014.

[18] M. Pizzonia, X. Clotet, F. Griscioli, G. Len, and E. Miciolino. D6.3 – Industrial Process-Related Threats Prevention and Detection Tool. Technical report, PREEMPTIVE, 2016.

[19] Security.nl. Disgruntled employee sabotages waste water processing facility. `https://www.security.nl/posting/404755/Werknemer+waterzuivering+VS+verdacht+van+sabotage`, 2014.

[20] ThetaRay. ThetaRay cyber-solution for Industrial sectors protecting critical infrastructure against unknown OT and IT cyber-attacks. `http://www.thetaray.com/`, 2017.

[21] A. Ursini, B. C. Villaverde, E. Costante, E. Zambon, B. Kassim, J. Kippe, and S. Pfrang. D7.3 – Context aware event analysis tool. Technical report, PREEMPTIVE, 2016.

[22] Wired. Feds: Hacker disabled offshore oil platform leak-detection system. `http://www.wired.com/2009/03/feds-hacker-dis/`, 2009.

[23] E. Zambon, A. Abbasi, K. Babatunde, S. Etalle, F. Griscioli, D. Lund, and M. Pizzonia. D7.3 – Host-based tools. Technical report, PREEMPTIVE, 2016.

END OF THE DOCUMENT