PREEMPTIVE

FP7 SECURITY 2013 - Grant Agreement No. 607093

Preventive Methodology And Tools To Protect Utilities

D4.3 PREEMPTIVE Methodology Evaluation Report

(01/04/2016 – 30/08/2016)

Deliverable Identifier:	D4.3
Delivery Date:	30/08/2016
Classification:	Public
Editor(s):	Kassim Babatunde, David Lund, Yakubu Tsado HWC
Document Version:	1.0
Contract Start Date:	March, 1st 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.

This deliverable has passed the SEC control according to the SEC members of the Preemptive Project.

Document Control Page

Title	D4.3– PREEMPTIVE Methodology Evaluation Report	
Editors	**Name**	**Organization**
	Kassim Babatunde, David Lund, Yakubu Tsado HWC	
Contributors	**Name**	**Organization**
	Jörg Kippe	IOSB
	Steffen Pfrang	IOSB
	Sinibaldi Giorgio	VITRO
	Amir Ribak	IEC
	Marco Sacchetti	UNIROMA3
	Berta Carballido	ENCS
	Andrew Buick	HARNSER
Format	Text – PDF	
Language	en-US	
Work-Package	WP4 - PREEMPTIVE Methodology Framework for utility networks	
Deliverable number	D4.3	
Due Date of Delivery	30/08/2016	
Actual Date of Delivery	24/01/2017	
Dissemination Level	Public	
Rights	PREEMPTIVE Consortium	
Audience	Public	
Date	January 24, 2017	
Revision	None	
Version	1.0	
Edited By	Kassim Babatunde, David Lund, Yakubu Tsado HWC	
Status	Project coordinator accepted	

Revision History

Version	Date	Description and comments	Edited by
0.1	January 10,2017	Draft version for peer review	HWC
0.5	January 16,2017	Second Draft review	HWC
0.8	January 19,2017	Third Draft review	HWC
1.0	January 24,2017	Final version	HWC

Contents

List of Figures

List of Tables

List of Acronyms - Definition

Acronym	Definition
ACL	Access Control
APT	Advanced Persistent Threats
CI	Critical Infrastructure
CII	Critical Information Infrastructure
D2.1	PREEMPTIVE deliverable D2.1 on "Taxonomy and Threat Analysis"
(D)DoS	(Distributed) Denial-of-Service
DPA	Data Protection Authority
EC3	European Cybercrime Centre
HMI	Human-Machine Interface
ICT	Information and Communication Technology
ICS	Industrial Control System
IDS	Intrusion Detection System
IED	Intelligent Electronic Device
IPS	Intrusion Prevention System
LIBE	EU Parliament Committee on Civil Liberties Justice and Home Affairs
OECD	Organisation for Economic Cooperation and Development
MITM	Man-In-The-Middle
MO	Modus Operandi (Method of Attack)
MTU	Master Terminal Unit
OMS	Outage Management System
PLC	Programmable Logic Controller
PRISM	Performance and Risk-based Integrated Security Methodology

Continues on next page

Continues from previous page

Acronym	**Definition**
RTU	Remote Terminal Unit
SCADA	Supervisory Control and Data Acquisition
VA	Vulnerability Assessment
VPN	Virtual Private Network
WP	Work Package
WS	WorkStation

Executive Summary

This deliverable is part of work package (WP) 4 PREEMPTIVE Methodology Framework for Utility Networks, which presents the report on findings of the PREEMPTIVE methodology evaluation on a real network utility environment. The purpose is to apply the risk assessment procedure defined in the previous work of deliverable D4.2 in order to assess the level of risk in a real network utility environment. The evaluation was carried out in a real gas utility network plant. The plant consists of both a gas distribution network and a heating distribution plant which makes use of gas for its heating. For the sake of bounding the evaluation effort, we focused just on the gas distribution network.

During the evaluation we exploit all possible ways for identifying critical assets and types of vulnerabilities that are present. The findings cover various stages of the risk assessment. The document is organised as follows: First we provide the description of the SCADA network at the evaluation site. Next we provide the objectives of the evaluation with regards to the corresponding stages of the same. Then we provide a detailed report of our findings for each risk assessment stage against the utility network. Lastly we discuss the suitability of the methodology approach to meet the needed cyber security challenges of the utility provider.

1 Introduction

The Industrial control system (ICS) is an integral part of a critical infrastructure. Its disruption can have severe consequence on the overall operation of a critical infrastructure (CI) in terms of security, economic well-being and reputational damage [1]. Critical infrastructures, comprising oil and gas plants, electricity generation plants, transportation systems and complex distributed systems are the backbone of any developed nation [2]. In most cases the ICSs is made up of a Supervisory Control and Data Acquisition (SCADA) system [3]. The SCADA system provides the overall monitoring and control of the industrial control system and its protection is highly important.

Part of the aim of the PREEMPTIVE project is to develop a methodology framework for utility networks to examine the security protection of the Critical Infrastructures which drill down to ICSs and its SCADA network as conducted in deliverable D4.2 [4]PREEMPTIVE Methodology reference. The methodology lays emphasis on procedures for conducting risk assessment in order to understand the risk to the utility. The PREEMPTIVE project addresses three utilities, which are electricity, gas and water [6]. The methodology framework is designed to be suitable for every critical infrastructure including those mentioned in the PREEMPTIVE project.

Our task in this deliverable is to evaluate the PREEMPTIVE methodology, by applying each procedure provided in the risk assessment to a real utility environment, and present our findings at the end of the evaluation. The evaluation was conducted in a gas utility network plant, consisting of two different sectors. The first sector is the main gas distribution for local end users while the other sector is the gas distribution for the heating plant. The gas in the heating plant is used for the heat production which is then sold to different households. The evaluation focused only on the gas distribution sector of the utility network for the sake of bounding the evaluation effort.

The evaluated gas plant has limited capability to fit into all aspects of our methodology procedures as the utility environment is small. For instance the visited gas plant is mostly made of physical components such as valves, pipelines, temperature gauges and pressure gauges, and they are not controlled via any ICT system present in the control center. Nevertheless, the evaluation target was to only focus on the cyber assets of the infrastructure. This decision made us pay attention to the ICT system within the control center and leave

the field devices out of our evaluation as no major cascaded risk is possible from the ICT system to the physical components.

This document is divided into 5 chapters. Chapter 2 of this document presents the description of the evaluation environment and the overall evaluation objectives. Here we describe each evaluation step in the risk assessment procedure. In chapter 3, we provide a description of our evaluation findings, including the steps taken during the evaluation and protection, and the targeted solution provided after the evaluation. Chapter 4 discusses the suitability of our PREEMPTIVE methodology to help meet the day-to-day cyber security challenges of the utility network. And lastly the concluding remarks are described in chapter 5.

2 Evaluation Process

In this chapter we present a description of the environment used for the evaluation and the evaluation objectives. The PREEMPTIVE methodology framework D4.2 [4] provides reference guidelines for improving security in critical infrastructures by assessing cyber risk and providing countermeasures. This helps to understand the threat and risk levels for an asset, and offers solutions for the protection for the critical infrastructure.

2.1 Overview description of gas plant SCADA network

In this section we present an overview of the SCADA network for the gas plant used for the PREEMPTIVE methodology evaluation. For security reasons, only a generic description of the evaluation plant is provided. The gas distribution plant is divided into two sections, the first section deals with the gas distribution for local end users and other gas utility users. The other section is responsible for gas distribution to the heating plant which is under control by the same organisation. The two environments provide us with different infrastructure choices.

As already mentioned, the evaluation focuses just on the gas distribution section. The gas distribution plant contain a SCADA network within the control centre of the utility company for monitoring the field devices operation as shown in figure 2.1. The same SCADA system is also used for controlling the level of gas distribution for the heating plant. It also provides alert notifications for the system administrator in case anything goes wrong on the field.
The SCADA network comprises of two types of Human machine Interfaces (HMI)s; (i) Fixed HMI and (ii) Mobile HMI. Both can perform the same functions depending on the level of access granted to the user. The fixed HMIs are installed and used within the premises of the gas utility distribution centre while the mobile ones provide the flexibility of accessing the site from a remote location via GPRS. Listed in table 2.1 are some of the primary assets that are genarally associated with SCADA network and are also identified during the evaluation.

The server used by the SCADA system is configured with redundancy which means that there is always a main server in active mode and another in listening mode. The purpose of this is that when the active server fails, the other listening server resumes the functions of the first server and vice versa. Two firewalls are in place in the network to protect the overall functionality of the network. The connection to the RTU and PLC is done via serial

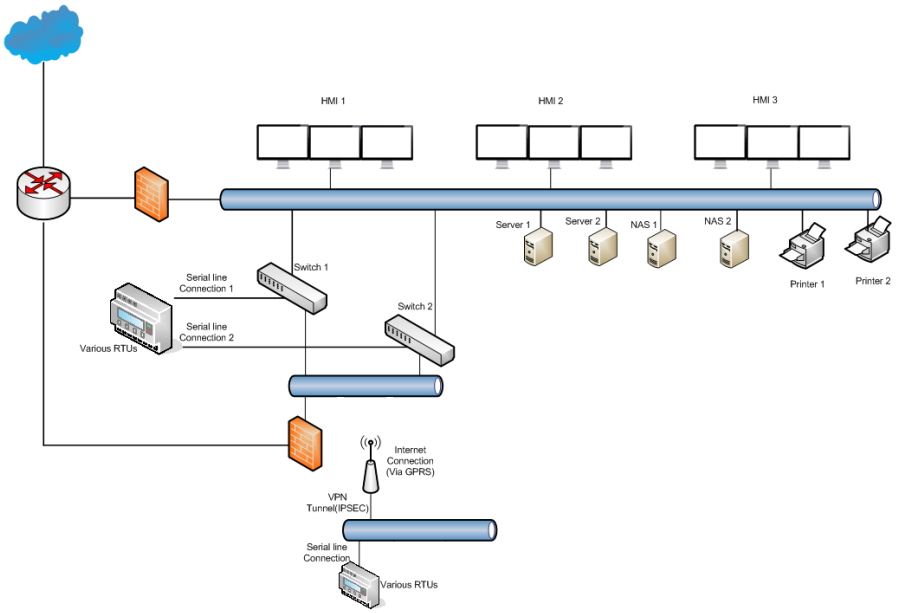

Figure 2.1: Gas distribution plant SCADA network

communications rather than an Ethernet connection. It is assumed that the whole SCADA network is isolated from the outside internet connection. So no regular updates are carried on any of the ICT components via the internet. The only internet connectivity is used for remote connection by the mobile HMI via GPRS.

Table 2.1: Primary Critical Asset.

Primary Asset	**Description**
SCADA servers	Provides overall remote monitoring and control of an ICSs
HMIs	Provides the visual interaction for operators to get access to remote devices
PLCs	Digital devices used in the automation of ICSs in the field

Continues on next page

Table 2.1 – *Continues from previous page*

Primary Asset	Description
Operating System	Software that manages the computer hardware and software resources and provide common interaction for different user either through GUI or command line

2.2 Evaluation Objectives

Our objective is to evaluate each step in the PREEMPTIVE methodology reference guide in a real system with an emphasis on the developed risk assessment guidelines and cybersecurity policy compliance.

The evaluation process aims at understanding the type of cyber security protection that has been put in place by the utility network provider to guide against present and future cyber attacks in their facility and how such attacks will affect or disrupt the operation of the utility. The key objectives of the evaluation process are described as follows;

- **Cyber Asset Characterization**: We aim to apply the asset identification procedure guideline to identify the critical cyber assets within the utility network. The asset identification also provides a guide for prioritizing each asset based on their criticality and potential of impact that affects the overall functionality and operation of the network utility.

- **Cyber Threat Assessment**: The second evaluation objective involves applying the threat assessment procedure. The threat assessment involves the identification of cyber threats that an attacker can leverage to carry out an attack on the utility network. This process also tries to categorize the threats based on their source. The next step in the threat assessment is applying several threat scenarios which the utility can be prone to after the identification of the threat sources.

- **Consequence Assessment**: The third evaluation objective involves applying the consequence assessment procedure. This procedure is used to ascertain the impact of threat or attack to an asset. Consequence scenarios are derived based on the impact of attack. Examples of consequence of a successful attack can be defined in terms of financial loss to the organization, operational loss of the SCADA operation and the reputational damage that arises due to the threat or attack to the facility.

- **Vulnerability Assessment**: The vulnerability assessment procedure follows the consequence assessment. The vulnerability assessment defines the flaws found in an asset that can used by an attacker in order to exploit the utility network. Several methods can be deployed by an attacker in order to gain knowledge of this weakness, including the use of an infected USB to create backdoor, port scanning, network sniffing through stolen network credential etc. Also different vulnerability tools can be used during the exploit of the network scanning of the utility network if the credential of network information is stolen.

- **Threat Likelihood Assessment**: The threat Likelihood assessment procedure is defined in terms of the possibility or intent that an existing threat is likely to carry out its objective within the utility network. The intent objectives could be the disruption of service and stealing of vital information. Our aim is to check if these possibilities can be achieved by an attacker. Examples of these possibilities are gaining access to the network infrastructure via an open port on a router or switch and re-configure the router or switch, also the possibility to gain access to the remote network access using stolen credentials and disrupt monitoring operation of the SCADA network.

- **Risk Assessment**:The risk assessment procedure is the last evaluation stage; this stage aims to look at the overall risk of each individual asset and provides the right countermeasure for each individual asset with higher level of risk. This procedure combines the outcome of three assessment stages, namely: Threat, Vulnerability and consequence to analyse the risk level.

3 Evaluation Findings During the Application of the Methodology

In this chapter we present the findings made during our evaluation of the PREEMPTIVE methodology when it was applied to an actual network utility. Here we present our general perception and observation of the network utility and what we think should be done based on the PREEMPTIVE methodology guidelines. The findings cover all the aspects of the risk assessment within our PREEMPTIVE methodology which is divided into different subsections.

3.1 Asset Characterization

During the process of the asset identification and ranking of the assets based on their criticality, we came across several findings. Some were obvious, some others interesting or even surprising. In the following, we will describe the findings and how we handled them.

- **Precise documentation**: The key to any asset characterization and identification is the prior knowledge about the existing critical infrastructure assets. You will need to get a precise documentation of the infrastructure and its assets in order to easily understand the infrastructure. That was a difficult part when conducting the asset identification. One problem we encountered is that the initial documentation was outdated because of changes that were not documented. In order to overcome this problem, it is necessary to find people that can tell you how the infrastructure really looks like. This process however does take a lot of time as you will need time and effort to understand the process and function of the assets one at a time.
- **Common understanding of an asset**: You will have to get to a common understanding of an asset. From the IT side, an asset might be a computing device that is associated with an IP or MAC address. From the production side, a whole machine including several computing devices is considered an asset, or in the other extreme, a box without any MAC or IP addresses might be a valuable asset for the CI. The definition of an asset will play a major role later on when dealing with the criticality of an asset. From a security point of view, communication protocols used in CIs are very vulnerable to attacks and thus could also be considered as an asset. We decided to list them in the asset list but did not evaluate them right now.

- **Information leakage**: Information about the critical infrastructures (CIs) (their assets and their processes) is to be kept secret by the utilitys owner because information leakage might pose security risks. You will have to come to an agreement on how to handle that situation. Without deep knowledge of the assets and processes, a risk analysis would be a very general guess. In conclusion, negotiating a NDA (Non-Disclosure Agreement) is a common practice when the assessment is performed by a third party.
- **Size of a company**: Mapping the network and the assets will require a very large effort in bigger companies/systems. In the instance of our evaluation, the complete understanding of the network topology required two days of interview and a visit to the physical sites. We admit that we were not that experienced in evaluation of CI, but it is obvious that the larger a CI is, the harder the challenge and it will take a lot of time when dealing with several people and visiting several, maybe even distributed sites.

3.1.1 Asset Ranking on Criticality

Asset criticality and ranking is another important step during the evaluation. You will expect that identified assets will have different levels of importance and functionality to the utility network. Therefore each asset can be ranked according to their criticality to the organisation operation. The utility operators are in the best position to provide information on which assets are critical to their operation.

3.1.2 Different aspects of criticality

Criticality scores are related to points of view. For instance, the assets may have different criticality if they are grouped by functionality instead of treating them separately (e.g. the power supply is critical, but its components taken separately are not). The criticality score represents different aspects that are often independent: outage time, replacement time, monetary cost. We decided to pay attention to that by using it as criterion for scoring. For example, if the average score of outage time, replacement time and monetary cost is high, we place such asset on the high critically score. If the average score is however low, then we assign low criticality to the asset.

3.1.3 Redundant assets

We discussed about scoring and ranking redundant assets as separate or as a single entity, as this has an impact on the criticality score. We decided to treat them as a single asset and

represent the redundancy by assigning them a lower criticality. The decision was based on the level of importance redundancy plays in asset robustness. If we consider the system as a whole (including the physical assets) then nothing is critical since there is always a manual backup/override. So we focused the cyber aspect and the availability of only the network. In this context, loss of operation means loss of SCADA network operation.

3.2 Cyber Threat Characterization

In our PREEMPTIVE methodology for threat characterisation, we focus mainly on identification of cyber threats that may pose a risk to either the physical or logical assets within the utility network. However after our visit to the utility network site, our findings shows that most of the physical assets are not logically controlled by the SCADA network (via Ethernet but serial communication).

We therefore decided, with the security expert team of the utility to focus only on cyber assets that can be affected by cyber threats or attacks to the functional operation of the SCADA network monitoring the critical infrastructure. In characterizing the threats during the evaluation, we observed that the majority of criminals are logical actors (Insider threats, competitors and amateur hackers) who look to achieve a favorable risk vs. reward ratio and select targets accordingly. Along with capability and intent of the threat actor, target attractiveness is therefore key in determining the likelihood of a cyber-attack against a specific SCADA network within the ICS, and requires an appreciation of both known vulnerability and consequences of impact.
It is also worth bearing in mind that some criminal groups such as foreign nations or expert hackers will conduct just as detailed vulnerability and consequence assessments as those done by the utility company when selecting their targets and methods of attack. In the case of our evaluation, our findings show that such utility might be of interest to such criminal group.

3.2.1 Threat Identification and Sources

During the evaluation of the PREEMPTIVE methodology we decided not to include non-criminal threats such as fire, earthquakes or any natural disaster as part of threat. Also physical security threats were neither considered, e.g. fence climbing with respect to the utility network. Our efforts concentrated on the primary grouping of the cybercriminal threats only. Based on our findings, the main threat source that is associated with the utility network is insider threat. Based on the discussion with the security team of the utility company, insider threats account for most of the threats that can be used to disrupt the operation of

the SCADA network since they can have direct access to the facilities. Other threats are related to organisation competitors, economical and foreign government policy. Although there are other cyber threats sources that we considered during the evaluation, we cannot place their impact within the utility company. An insider, such as staff or visitor to the plant, can create a backdoor for an attacker to gain network access into the utility company by planting spyware/malware in the organization computer system.

When assessing the sources of threat in this particular ICS, it was judged that the predominant threat sources were Insiders, Script Kiddies or Inadvertent damage. Descriptions of these are as follows:

- **Insiders**: We considered the insider threat has a number of possible actors that include staff, contractors, former employees and visitors. The disgruntled individual remains the most dangerous threat source within the insider category as the insider often has good knowledge of the target facility combined with unrestricted access. Moreover, it does not necessarily have to be an expert in cyber-crime in order to cause damage. Such person can also be used to create a network backdoor for network hacking of the SCADA system.

- **Inadvertent Damage**: Often associated with Insiders, careless or inadequately trained staff and poor cyber security procedures can accidentally cause damage and disruption to networks and facilities, for example by the introduction of malware into systems through the use of infected USB device. This type of threat can be common in organization where there is no security policy in place.

- **Script Kiddies**: A person who has the knowledge of using existing computer scripts or codes to hack into computers network, lacking the expertise to write their own, example of this is malicious JavaScript or SQL script.

3.2.2 Threat Scenarios

The process involves defining different possible scenarios for attacking specific assets based on the threats identified. The scenario definition can also be associated with techniques and tools used during the attack. With the three threat actors we identified during the evaluation, it was decided that some method of attack applicable to the utility network could be defined with the help of the organisation staff. The definition of threat and attack scenarios was based on objective opinion on how the known threats can be leveraged in order to achieve disruption to the SCADA network. Some of the considered attack scenarios are listed below;

- **Information theft**: This is carried out with the help of an insider and possible scenarios that can take place are:
  - By inserting a USB device into an accessible computer system to steal information about the organization operation and configuration.
  - Also such stolen information can be sold to rival competitors in order to improve their business.
  - Remote Access: A backdoor remote access can be created with network connection credential
  - Disruption of Operation: This also is associated with insider help, if malware is planted in the HMI machine, such malware can cause disruption to the monitoring and control of the SCADA system.
  - Service disruption of the SCADA server is major catastrophe; this will bring the whole SCADA operation to an alt.
- **Amateur Hacker**: This is carried out by outsiders learning how to perform hacking and possible scenarios that can take place are:
  - Knowing/Unknowingly cause Denial of Service while trying the existing computer hacking code
  - Knowing/Unknowingly gain remote access connection to the remote site of the organisation
  - Knowing/Unknowingly gain access to vast information about the configuration of the organisation system.

3.3 Consequence Assessment

Consequence assessment is defined in terms of the impact of threats to an asset. Our evaluation at this stage is conducted based on the previous knowledge of identified cyber assets within the utility network. Each cyber asset is paired with a threat scenario based on known threat in order to ascertain the level of damage that such threat can have on the utility network. In some cases, we ruled out some threat scenarios due to the absence of any tangible consequence to the utility network.

During our further analysis, scoring consequence criteria that we defined before the evaluation is adjusted based on the impact level of the pair instances. For example, considering a scenario where a server of the ICS System has a degree of resistance to DDOS attack and would not necessarily be overwhelmed as a result, this would have none or less significant

consequences on the network.

3.3.1 Consequence of Attacks on Identified Assets

The aim of an attacker is to cause partial disruption, total disruption or stealing of vital information on the SCADA network. So we decided to look at different attacks that might have higher significance to a SCADA network based on the different threats we identified during the evaluation. During the consideration of the consequence, the security team of the utility provided some indications on the impact of the threat to their organisation. The attacks can be of the form listed below which are based on identified threats during the threat assessment.

- Access the information for obtaining data for commercial or criminal usage. These are relevantly simple attacks if an insider provide access information to an attacker and the damages may be limited to financial consequences. Our findings show that the amount loss by the organization in this regard can only be measured based on level of information that was obtained by the attacker.
- Data manipulation for gaining economical advantage or for disrupting service. These are complicated attacks requiring knowledge, time and monetary funding. They are usually related to some kind of man-in-the-middle (MITM) attacks and require deep penetration and access to the system. Our findings show that this type of attacks is of higher consequence to the organization which can cause not just financial damage, it can also lead to reputational damage and loss time of operation.
- DoS attack for service disruption. These are basic and common attacks with limited implications and limited effects. It's usually time limited and the consequences are related to reputation and some financial lose. We observed that if a DoS attack is carried on the network, it does not really affect the entire system as manual override is available for field devices. However if we consider just the SCADA network only, the operator will not have access to monitoring and control of the field device.

The consequence of these attacks can vary based on the level of existing protection that is already in place before the attack. Examples of such protection includes firewalls, access control policies, antivirus protection etc.

The consequences can have different impact on the level of operation to the utility network provider. During the evaluation of the utility, we based the consequence evaluation on three major factors which are: organisation reputation, financial loss and operation time loss. The

security experts found those three important to their organisation. The three factors are then used to categorise some of the consequences of attack on the SCADA network as follows;

- Low impact, short time and minimal financial damages. Usually it entails low recovery time and very light damage if any at all, and requires very simple procedures to bring to the original situation as before the attack. This situation is preferable since the recovery process is very cheap and involves minimalistic resources financially and logistically.
- Medium impact, in a general point of view (include financially and logistically), these kinds of attacks are quite common and their effects are limited (in the final damage they cause). The cost and consequences of this kind of attacks totals with not so high sums of money and some issues of reputations to the organization in term of business partners (local businesses) or customer (end user).
- High impact in general point of view (include financial, logistic and time operational loss) this kinds of attack are not common, but when it happen their effects are vast (in the final damage they cause). The cost of cosequences of this kind of attacks totals with higher sums of money compare to the medium impact, loss of time of operations and issues of local reputations to the organization in term of business partners(local busniesses) or customer (end users).

During the interaction with the security team on site, we concluded that there is minimal or no international reputational damage to the organization since their operation is based on local region level only.

3.4 Vulnerabilities Identified in Asset

The vulnerability assessment process is another key process in risk assessment. This is defined in terms of the level of weakness or opening that an attacker may use in order to exploit the utility network to carry out a cyber attack. Several methods may be employed by an attacker in order to check the vulnerability of such utility ranging from port scanning, network sniffing, password guessing etc. The vulnerability assessment with regards to cyber security and resilience is based on four core factors which are Prevention, Detection, Delay and Response. The summation of those factors is what helps determine the vulnerability of any cyber system. During our evaluation process of the test plant we observed that it was difficult to build a metric summation account for the vulnerabilities using all the factors listed above.

We therefore agreed and decided with security expert of the utility provider not to consider the four factors. The reason for this is that the four factors presented the same criteria for

scoring which does not fit the utility needs. Therefore, we finally decided to estimate the vulnerabilities by assigning a score threshold to them and list them as per below:

- We chose to keep the list short by pointing out broad categories of vulnerabilities (e.g. Servers run the obsolete windows server 2003 instead of Servers have security vulnerabilities MS1002, MS2006, MS3826, MS8364...). Part of our findings is that the organisation does not have any maintenance agreement for any of the servers
- Also the workstations used for the monitoring and control are also vulnerable to different known attacks and also close to its end of life (EoL). There is no more software supported update for the operating systems.
- During the vulnerability assessment our findings also observed that, the workstations did not have any security policy to protect against the use of the USB on any of the work stations. This is another vulnerability which can be easily accessed by an outsider if they have access into the premises of the organization.
- All the antivirus on the workstations are not updated regularly which makes them vulnerable to zero day attacks
- We also observed that the present network configuration is managed by service providers and the organisation in itself does not know or have access to the configuration setting or provide an extra layer of protection for their network. This implies that, if the network is down or under attack, they will rely solely on outside help rather than internal help.
- We also observed that some of the networking equipment had access to web services; this makes them vulnerable to a network attack.
- We chose not to discuss the PLCs (and all the low level operational components) because:
  - Even if the connection goes down or the SCADA is affected they operate autonomously
  - The only way to affect them is locally by means of altering the telegrams that are exchanged between the PLCs and the RTUs
- Since we do not have numeric statistics, we have limited insights about the vulnerability scores and we assigned them based on our opinion and expertise. In a real scenario the company would probably assign this task to someone capable of assessing the scores in a better way. We also chose to assign only the overall vulnerability score and keeping the single scores (detection, response, delay, prevention) out of scope.

3.5 Protection Objectives

The main input source for the identification of protection objectives is the risk register. One of the findings of the evaluation is that some protection objectives would not have been clearly identified by only looking at the risks register, because those objectives do not refer to single assets, but instead they refer to lack of security and business procedures (e.g. a business continuity plan).

This is due to the fact that the assets are defined as concrete elements and not abstract processes like policies and procedures (or lack of them). In the asset identification and vulnerability assessment of the PREEMPTIVE methodology there is emphasis on technical aspects, while during the protection objectives definition phase, the methodology defines countermeasures as both concrete tools and procedural policies. The method for generating the protection objectives is indicated as:

- look at the risk register
- select the risk scenarios above the acceptance threshold
- For each scenario, describe in short form the objective of any mitigation measure that could be applied.

While this is very straightforward for many risk scenarios, where a technical solution (e.g. the deployment of a specific tool) is easily found by a security expert, some scenarios depend on the absence of some kind of policy in the business process of the utility. Policies are discussed in the PREEMPTIVE methodology in relation to the adoption of the PREEMPTIVE tools and the filling of existing gaps in other standards, but they can be important also for the generation of the protection objectives.

A possible approach to identify missing policies and procedures could be:

- Look at both the countermeasures categories and the PREEMPTIVE policies, and try to determine if each one is relevant to the considered risk scenario.
- From those broad guidelines one can identify the deployment of policies and procedures that could be included in the protection objectives (e.g. the establishment of a business continuity and incident recovery plan).
- The knowledge of previous standards can also be helpful in defining which cybersecurity policies should be implemented in the utility process.

The inclusion of policies and procedures in the protection objectives could help in mitigating entire categories of risks instead of specific technical countermeasures that address single risk scenarios.

3.5.1 Solution provided to the Utility to Enhance Protection against Cyber Attacks

The protection objectives are the first input for the utility decisions about the deployment of risk mitigation measures. They indicate at a high level what should be done in order to mitigate the risk associated with a particular scenario.

Since both the technical department (in charge of implementing the countermeasures) and the utility management (in charge of deciding the course of action and providing the necessary resources) are interested in the risk assessment outcomes, a single document stating the protection objectives may not be the best fit for the needs of the two parties. To make the protection objectives more useful, a possible approach could be to:

- define the protection objectives
- for each protection objective, define countermeasures with a number of different concrete implementation options
- Rank those options by effectiveness from the risk mitigation point of view. They should be detailed enough in order to reach two goals:
  - help the technical department with their implementation
  - Provide the management with enough data to assess and estimate their deployment costs.

The utility management (at least in case of small to medium companies, the ones free to spend their budget as they decide) can then evaluate each option with the insight of the technical department and choose the specific countermeasures that best fit the utility needs, considering financial and other implementation costs. Where the proposed countermeasures cannot be deployed because of the associated costs, or if they only partially achieve their goal, the protection objectives should be reviewed and updated accordingly. Feedback from the utility could also be of great advantage for the person defining the protection objectives, to refine the selection of countermeasures, as well as to assess the implementation feasibility and costs associated with each one of them.

3.6 Security Policies

The security policy and compliance is an important part of any critical infrastructure. It is necessary for any ICS to comply with a set of security guidelines in order to protect its infrastructure against cyber attacks. During the evaluation, the interaction with the security

team of the utility company provided us with insight to the level of security policy that was put in place to protect their facilities against cyber attack. However our findings indicate that little or nothing is done to improve the security policies as the decision makers of the organisation see no reason for the improvement. Due to sensitivity of this evaluation, the security policies are not mentioned in any part of this document. Some security policies were then suggested based on the PREEMPTIVE methodology such as USB policies, extra layer of firewall controlled by the utility themself etc.

4 Suitability of PREEMPTIVE Methodology to the Evaluated Utility

The PREEMPTIVE methodology provides guidelines for assessing and conducting risk assessment. The risk assessment is part of the common practise for measuring the level of countermeasures required by different organisations for the protection of their assets against cyber attacks. In this chapter we describe the suitability of PREEMPTIVE methodology in providing the necessary guides required by utility network providers.

4.1 Asset Characterization and Identification

PREEMPTIVE methodology approach for asset characterisation and identification provides the in-depth analysis view of the critical asset in terms of importance of such an asset to the organisation. The overall assessment process helped the utilty to understand the interrelationship of the IT-related assets to the physical assets. During the evaluation, only IT components of the utility network provider were identified and characterised based on their criticality. The approach also helped in providing the necessary information on how IT components affect the overall physical operation of the utility network.

4.2 Threat Characterization

The threat characterisation approach in PREEMPTIVE methodology provided a wider and in-depth analysis for the utility provider during the evaluation procedure. The threat characterisation approach helped the utility provider to know and understand where a cyber threat can originate from within their operational environment. Since much of the focus of the characterisation is on cyber threats, different threat scenarios were defined during the evaluation relating to the current threats faced by the assets. Future threats and how the threats can impact the related cyber asset are analysis. The procedure helped the utility provider to understand the hierarchy in threat level and the damage such threat can have on the entire operation of the SCADA operation.

4.3 Consequence Assessment

The consequence assessment approach in PREEMPTIVE methodology also covers vast areas on possible impact to the utility provider. The approach helped the network providers to understand the impact level of certain threats and attacks to their facilities. The process provided the several possible consequences which forms the base of loss to their facilities in term of reputational damage and financial implication to their organisation. The suitability of this approach is that it helped the technical expert understand that if certain precaution is not taken to protect against the existing threats, an attacker might use it against them and the consequence of such act will be severe.

4.4 Vulnerability Assessment

The vulnerability assessment approach in the PREEMPTIVE methodology covers a wide area of possibilities for vulnerable components that can be encountered in critical infrastructures; this includes the control centre, communications networks, field devices and equipment. We limited our scope during the vulnerability evaluation to the control centre due to structure and topology of the infrastructure. The process helped identify several vulnerabilities within the control centre of the utility network. The vulnerabilities included software usage such as sufficient malware protection, access control, default password configuration and the network configuration. The procedure provided the utility management a better view of what should be considered vulnerable when it comes to cybersecurity.

4.5 Threat Likelihood

The threat likelihood assessment approach in the PREEMPTIVE methodology provides guides on how to understand that certain types of cyber threat can have the capability to carry out attacks on specific utilities. This capability is determined based on different circumstances such as the level of difficulty on gaining access to utility site, existing countermeasures that are in place, geographical location where the site is located. The other part is the attractiveness of such utility provider asset to cyber attacks. During the application of this stage of procedure to the utility, we found out that though some vulnerability does exist in the site, the possibility or capability for such asset to be attacked is minimal when we based our subjective opinion on the location of such utility.

So when we consider the entire likelihood factor based on the utility, the possibility of cyber attack to the utility is minimal.

The procedure was able to provide a objective in-depth analysis of the likelihood of future intent that might warrant an attack to the utility. An example of such intent is when an amateur cyber-hacker is learning how to gain access to SCADA network; he/she might consider a small scale environment for practice. At the end of this stage we saw that the end user was also able to understand what is needed to be put in place in case of future intent of attack due to low cyber security measure that are in place at the time of evaluation. Also the utility provider saw this stage very vital to them in order for them to protect assets that might be easily visible to attack such as the USB.

4.6 Protection objectives

The protection objectives approach in the PREEMPTIVE methodology communicates to the utility the elements in the ICS that have been identified as the most critical by the risk assessment, together with the strategies needed to lower or eliminate the associated risks. Having a list of objectives sorted by criticality allows the utility to focus resources on the most important elements of the infrastructure. This approach gives the utility management a clear representation of the required cybersecurity objectives that need to be reached, preparing the ground to choose the concrete countermeasures to implement. While giving sufficiently specific guidance on the steps needed to raise the security of considered assets, this approach leaves room for the utility management to follow any established procedure or policy to choose the set of countermeasures to be implemented and to assess their associated risks and benefits.

5 Conclusion

In this deliverable, we provided the outcome of our findings when applying the PREEMPTIVE methodology to a real utility network environment. The evaluation was conducted in gas distribution utility plant composed by a gas and heating distribution plants. As part of the evaluation process, we visited the gas distribution plant of the utility network in order to understand the operational environment.

Significant issues that were noted from the first stage of the evaluation process included: (i) Lack of proper documentation of the infrastructure, (ii) Lack of proper troubleshooting procedures in case anything goes wrong in relation to a cyber attack. (iii) Agreement on what assets should be addressed and categorised.

Several types of cyber threats were discussed based on the infrastructure, threat scenarios that an attacker can use to gain access to the utility company based on the known threats were defined. The impact of threats/attack from the defined threat/attack scenario proved key to improving the utility providers understanding of the imminent danger that may be faced by their network.

PREEMPTIVE methodology provided the necessary countermeasure needed to enhance the cyber protection of the utility provider system. The countermeasures include, among others: (i) the provision of USB security policies which will guide on how to safely use USBs within the organization; and (ii) guidelines to protect against DoS attacks by limiting their level of impact.

This document was organised into five chapters: Chapter 2 provided the description of the evaluated utility plant. The idea was to have information on the environment used. The overall objectives of the evaluation were discussed, in this chapter we listed and explained each stage of the risk assessment process.
The findings made during the evaluation were presented in Chapter 3; these findings cover all the stages in the risk assessment which are asset characterisation and identification, cyber threat characterisation, vulnerability assessment, consequences assessment, threat likelihood assessment, threat assessment and protection objectives. The last part looks at the security policies within the organization The suitability of PREEMPTIVE methodology was described

in Chapter 4 based on the outcome of our evaluation findings. In this chapter we explained how each stages of the methodology helped in the analysis of threats faced by utility network and how useful our approach was to the utility management of the organization.

Bibliography

[1] ENISA – European Union Agency for Network and Information Security. Critical Infrastructures and Services. https://www.enisa.europa.eu/topics/critical-information-infrastructures-and-services, November 2016.

[2] HARNSER. Prism – a reference security management plan for energy infrastructure, December 2011.

[3] ISO/IEC – 27005 International Organization for Standardization and the International Electrotechnical Commission. Techniques-information security risk management. Technical report, December 2011.

[4] 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.

[5] B. Sandro, F. Alessandro, and M. Maurizio. The importance of securing industrial control systems of critical infrastructures. http://www.nonproliferation.eu/web/documents/other/sandrobolognaalessandrofasanimauriziomartellini516291dea8ac8.pdf, December 2013.

[6] E. Zambon, I. Cairo, E. Costante, M. Guadagnoli, D. Lavernia, G. E. Leon, J. L. Marin, B. R. R. Regis, A. Ribak, A. Ruiz, and L. Trilla. D2.3 – Reference Taxonomy on Industrial Control Systems Networks for Utilities. Technical report, preemptive, 2015.

END OF THE DOCUMENT