FP7-610416-PANOPTESEC

Dynamic Risk Approaches for Automated Cyber Defence

D2.2.1: Operational Requirements

Work-Package	WP2	Deliverable	D2.2.1
Due Date	27-03-2015	Submission Date	27-03-2015
Main Author(s)	Nicolas Prigent (CentraleSupélec)		
Contributors	All project participants		
Version	V2.1	Status	Final
Dissemination Level	PU	Nature	R
Keywords	Operational, Requirements, Methodology		

Part of the Seventh

Framework Program

Funded by the EC - DG Connect

EXECUTIVE SUMMARY

This document presents the Operational Requirements for the PANOPTESEC system. Its purpose is to define the functional and non-functional requirements that will guide the whole PANOPTESEC project.

First, we present the methodology used to identify stakeholders and elicit, analyze, model, trace, validate and manage requirements. Then, we provide a brief description of the PANOPTESEC system and identify client, market, partner and user stakeholders. Actors (persons and non persons) are identified and users characteristics are detailed.

Three user scenarios are also provided that cover the PANOPTESEC application domains. The first user scenario describes the course of action during an attack against the Command & Control systems of a critical infrastructure. The second user scenario describes the course of action during an attack against SCADA equipments/devices of a critical infrastructure. Finally, the last user scenario describes the course of action during an attack against nodes that operate ICT services underlying a business process. For each of these scenarios, the behaviours of the PANOPTESEC system and of its operators is described.

Finally, we describe the functional and non-functional requirements that were identified. Functional requirement are organized in five categories (Data Sources and Collection, Information Correlation and Abstraction, Proactive Response, Reactive Response and Visualization) according to the high-level functionality of the PANOPTESEC system they relate to. Following the ISO 25010:2011 standard [2], non-functional requirements are organized into seven categories: Performance/Efficiency, Compatibility, Usability, Reliability, Security, Maintainability and Portability.

This document will be used all along the PANOPTESEC project as the baseline for the features the PANOPTESEC system must provide. It will guide design and development and will be used at the end of the project to evaluate its results.

HISTORY

Version	Date	Name/Partner	Comment
V1.0	30-04-2014	Nicolas Prigent/ CentraleSupélec	Previous version of the document.
V1.1	11-01-2015	Nicolas Prigent/ CentraleSupélec	Initial creation of the new version of document.
V1.2	17-01-2015	Giuseppe Santucci, Marco Angelini & Silvia Buonomi / U. Roma	Changes to the organization of the document so as to fit **IEEE 830-1998 Recommended Practice Software Requirements Specifications**
V1.3	12-02-2015	Andrea Guarino/ACEA	Description of ACEA and User Characteristics.
V1.4	16-02-2015	Matteo Merialdo/REHA	Added requirements.
V1.5	19-02-2015	Giuseppe Santucci /U.Roma	Modification to section 2 Methodology.
V1.6	28-02-2015	Giuseppe Santucci /U.Roma	Modification to section 2 Methodology, user roles suggestion on Section 3, and section 7 References.
V1.7	05-03-2015	Nicolas Prigent/ CentraleSupélec	Integration of user scenarios and functional requirements. Inclusion with the updated template.
V1.8	08-03-2015	Nicolas Prigent/ CentraleSupélec	Integration of non-functional requirements.
V1.9	11-03-2015	Nicolas Prigent/ CentraleSupélec	Goals and Main Purpose, User Scenarios integration.
V1.10	14-03-2015	Nicolas Prigent/ CentraleSupélec	Non-functional requirements goals and main purpose totally integrated.
V1.11	16-03-2015	Nicolas Prigent/ CentraleSupélec	Last integration before quality assurance.
V1.12	20-03-2015	Nicolas Prigent/ CentraleSupélec	Modifications following comments made during quality assurance. Especially, Stakeholders and User descriptions have reorganiazed to make them clearer and the whole requirements sections are now in portrait orientitation.
V1.13	22-03-2015	Nicolas Prigent/ CentraleSupélec	Modifications following comments made during quality assurance. Especially, updating user scenarios.
V1.14	23-03-2015	Nicolas Prigent/	FP7 and DoW Objectives inserted. User Scenarios

		CentraleSupélec	made clearer.
V1.15	25-03-2015	Nicolas Prigent/ CentraleSupélec	Final version before final review.
V2.0	26-03-2015	Nicolas Prigent/ CentraleSupélec	Final version.
V2.1	27-03-2015	Douglas Wiemer/RHEA	Final version, minor typo corrections.

TABLE OF CONTENTS

TABLE OF FIGURES

LIST OF TABLES

ACRONYMS AND DEFINITIONS

Acronym	Meaning
ACEA	ACEA S.p.A.
ADD	Attribute-Driven Design
ALBLF	Alcatel-Lucent Bell Labs France
ASR	Architecturally Significant Requirement
C&C	Command and Control
CC	Change Control
CI	Configuration Item
CIS-UROME	Università Degli Studi Di Roma La Sapienza
CM	Configuration Management
DoW	Description of Work
DR	Design Review
EPIST	Epistematica SRL
IaaS	Infrastructure as a Service
ICS	Information and Communication System
ICT	Information and Communication Technology
IDS	Intrusion Detection System
IMT	Institut Mines-Telecom
MOM	Minutes Of Meeting
PR	Peer Review
QA	Quality Assurance
QAM	Quality Assurance Manager
QR	Quality Review
QRSR	Quality Review Summary Report
RB	Requirement Baseline
RHEA	RHEA System S.A.
SCADA	Supervisory Control And Data Acquisition
SDLC	Software Development Life Cycle

SUPELEC	Ecole Supérieure D'Électricité
SVN	Subversion Repository
TPM	Technical Project Manager
UoL	Universität zu Lübeck
WBS	Workpackage Breakdown Structure
WPL	WorkPackage Leader

Table 1: Acronyms and Definitions

1 INTRODUCTION

1.1 Context

As dependency has grown on networks and computer systems, so have the motives and capabilities of cyber adversaries to attack them. Regardless of their motives, cyber attackers are often able to penetrate networks and computer systems to extract valuable information (compromising confidentiality), tamper with the accuracy of the information (compromising integrity) and overload or otherwise prevent access to needed services and systems (compromising availability). Any of such tactics used by the cyber adversaries can have significant negative impacts on an organization's business, reputation and liabilities. In the era of open networks and platforms, pioneered by paradigms such as the internet, web services, cloud computing and mobile computing, attacks find more venues to exploit the complexity and scale of use to cause increasingly substantial damages.

The objective of the PANOPTESEC consortium is to deliver a beyond-state-of-the-art prototype of an automated cyber defence decision support system that is intentionally designed to meet FP7-ICT-2013-10 Objective ICT-2013.1.5 Trustworthy ICT item (c). That is, the PANOPTESEC consortium will deliver an operational prototype as a means to "prevent, detect, manage and react to cyber incidents in real-time, and to support breach notifications, improving the situational awareness and supporting the decision-making process" required by cyber operators. "It will also develop and demonstrate advanced technologies and tools that will empower users, notably individuals and SMEs, in handling security incidents".

This document presents the operational requirements that apply to the PANOPTESEC system. Its objective is to provide a baseline for the PANOPTESEC system.

1.2 Purpose

The purpose of this deliverable is to present the operational functional and non-functional requirements for the whole PANOPTESEC system. The methodology followed by the PANOPTESEC consortium for requirements elicitation, analysis, modeling, traceability, coverage and management is presented. Then, stakeholders and actors are identified and three user scenarios are presented to help better understant the context of use of the PANOPTESEC system. Then, functional an non-functional requirements are presented.

1.3 Scope

The scope of this deliverable is first to ensure that all contributors to the PANOPTESEC project share a common view of its objectives. To that end, this deliverable identifies stakehloders, actors, operational context and course of action.

Second, this deliverable serves as a basis to define functional and non-functional requirements for the various components of the PANOPTESEC architecture and of the PANOPTESEC architecture itself. It be used all along the PANOPTESEC project to guide decisions and decide priorities. At the end of the PANOPTESEC project, this document will be used to assess its results.

1.4 Document Structure

This *D2.1.1: Operational Requirements* deliverable is structured in the following manner:

Section 1 Introduction: Describes the context, purpose and scope of the deliverable.

Section 2 Methodology: Describes the methodology followed in the development of the deliverable. Specifically, stakeholder identification as well as requirements elicitation, analysis, modeling, traceability, validation and management are presented.

Section 3 The PANOPTESEC system: Decribes the PANOPTESEC system and the high-level functions it should provide according to the DoW [13].

Section 4 Stakeholders identification: Present the client, market, partner and user stakeholders.

Section 5 Actors and user characteristics: Present the actors that have been identified and describes the user characteristics.

Section 6 User scenario: Presents three user scenarios that cover the application context of the PANOPTESEC system.

Section 7 Functional requirements: Presents the identified functional requirements, grouped by the high-level functionality the relate to (Data Sources and Collection, Information Correlation and Abstraction, Proactive Response, Reactive Response and VIsualization).

Section 8 Non-functional requirements: Presents the identified non-functional requirements. Following the ISO 25010:2011 standard [2], non-functional requirements are organized into seven categories: Performance/Efficiency, Compatibility, Usability, Reliability, Security, Maintainability and Portability.

Section 9 Conclusion: Summarizes the findings, results and recommendations.

Section 10 References: Lists the documents refered to.

2 METHODOLOGY

The methodologies and technologies developed in the context of a European project are quite different from the existing solutions that are targeting industrial projects. In the PANOPTESEC project, to collect requirements and design and implement software, we use a best practice that encompasses the integration of two highly usable and effective approaches that are: the spiral life cycle model and the use of user-centered design (UCD) techniques. CIS-UROME has used parts of this model successfully in many FP6 and FP7 European research projects such as WORKPAD and SM4ALL.

The spiral life-cycle [6] is an iterative process. It starts with initial requirements gathering. This phase is followed by rapid propositions on new basic research ideas, design, and development of a prototype implementing them. This prototype is then tested and validated by the users and is enhanced in the next iteration with users feedbacks and

additional requirements. The test results provide a new set of requirements that redefine or complete the old set. With the second set of requirements, a new design and development phase is performed. After that, users are required to test the system again.

The PANOPTESEC Consortium wants to involve stakeholders in the process of research, development and prototype creation and introduction. According to this objective, the PANOPTESEC prototype will be developed by using a user-centered and participatory methodology. User-centered design (UCD) methodology places end-users (as opposed to the developped object/system) at the center and involves them in design and development activities [5][7]. It is a design philosophy that focuses also on cognitive factors (such as perception, memory, learning, problem-solving, etc.) as they come into play during people interactions with objects and/or systems. It seeks to answer questions about users and their tasks and goals, and further on using the findings to drive development and design. This is done, for example, by representing or modelling users in **scenarios**, having users **testing prototypes** (either paper or working prototype), and involving users in **design decisions** (e.g., thorough participatory design). The activities in UCD methodology aim at reducing the risks of the software project and increasing the overall product quality [7]. The standard *ISO 9241-210:2010: Human-centered design for interactive systems* [3] provides guidance on user-oriented design process for including human-centered activities throughout a development lifecycle.

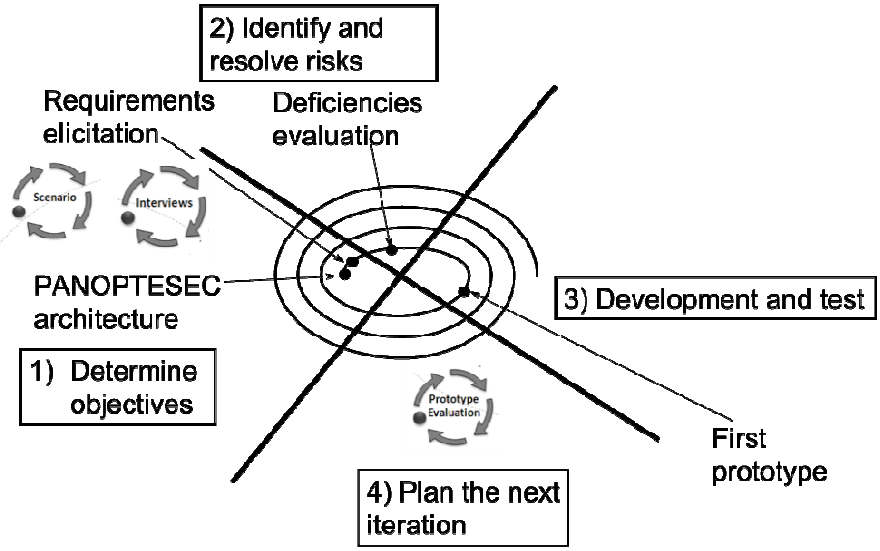

Figure 1: The PANOPTESEC UCD lifecycle

Figure 1 sketches the spiral lifecycle used to model the PANOPTESEC development. The spiral describes the four main macro-activities, detailed in the following:

1. **Determine objectives**. The purpose of this step it to determine objectives, alternatives, and constraints. According to the design of complex systems that rely on a shared knowledge of best practices and standard, the starting point for

collecting requirements from the stakeholders was the FP7 ICT 1 5 item c [14], the PANOPTESEC DoW [13] and the PANOPTESEC High-Level Preliminary Design [10] that includes and specializes concept available in the standard ISO/IEC 27001 - Information security management [4]. This body of knowledge has been used to collect the set of operational requirements described in this deliverable. To this aim, requirements elicitation has been performed through **interviews**, **scenarios**, and the definition of **user profiles**.

2. **Identify and resolve risk**. This is a standard software engineering activity, in which potential risks are evaluated and assessed against mitigation actions. A starting point in the risk analysis is the identification of current deficiencies in the current automated cyber-defence decision support. The result of this work can be found in D.2.2.1 Deficiencies Evaluation.
3. **Developement and test**. This step is devoted to the implementation and test of software prototypes whose maturity depends on the number of iterations. End users are involved in this phase, clarifying design and implementation issues. Artifacts produced in this phase are demonstration prototypes, used both for validating existing requirements and for collecting new ones.
4. **Plan the next iteration**. This step assesses what has been done in the iteration and uses this information to plan and drive the next iteration. Users are again involved in the activities, evaluating prototypes and providing feedback.

2.1 Stakeholder identification

Stakeholders represent any person or entity that may be affected by or may affect the scope and intended use of the system or software developed in the PANOPTESEC project. Stakeholders are identified under the following categories:

1. Client stakeholders: Client stakeholders represent those organizations or agencies for which there is a contractual relationship. In the case of the PANOPTESEC project, the client stakeholder is the European Commission.
2. Market stakeholders: Market stakeholders represent the various market segments wherein the resulting product, system or software may be sold. Commonly, the market stakeholders may be driven by the product marketing organization or derived from existing clients and market analysis and study. In the case of the PANOPTESEC project, the market stakeholders are driven by the anticipated exploitation plans of the partners and by the requirements identified through the external advisory board (EAB).
3. Partner stakeholders: Partner stakeholders represent the requirements of the participant organizations represented by the delivery team. Partners may influence requirements due to particular plans for research direction and outcomes, development plans or technology solutions, personnel development and training, as well as, eventual exploitation plans.
4. User stakeholders: User stakeholders represent the business owners and system or software operators of project. They may already be identified as Client, Market or

Partner stakeholders. However, User stakeholders are more tightly coupled to the specific development activities and drive user interface and feature requirements. In the case of the PANOPTESEC project, the user stakeholder is ACEA.

It is the responsibility of the leader assigned for overall system requirements (i.e., the WP2 Leader) to ensure appropriate stakeholders have been identified and engaged in the project.

2.2 Requirements elicitation

The Work Package Leader (WPL, or their assigned representative) communicates with the stakeholder or user to understand operational needs and requirements, making sure to record the results.

Requirements are identified according to the following criteria:

- Develop high-level operational user scenarios that describe the use of the proposed system or software. The description is recorded using the PANOPTESEC Scenario Template [16];
- Identify stakeholders and user roles;
- Identify high level objectives and goals;
- Identify operational capabilities of the system or software;
- Identify system or software component requirements;
- Identify non-functional requirements (performance, efficiency, compatibility, usability, reliability, security, maintainability, and portability); and
- Identify design constraints.

2.3 Requirements analysis

The WPL (or their assigned representative) then analyze the intended use of the product to be developed.

Top-level product and component requirement items (software) are identified in accordance with the Work packages Breakdown Structure (WBS). Based on such initial understanding with the client the project charter is prepared.

Requirements are then identified and allocated to task list.

Requirements are documented in the Functional Requirements Document and/or Project Charter document. The BA head will ensure that all top level product requirements, product component requirements are clearly addressed by the high level requirements to ensure that all requirements have been addressed and satisfied.

It includes the following elements in the requirements document, as applicable to the level of details intended by the work product (e.g., operational vs. functional requirements, high-level vs. detailed) and as they apply to the project:

- Product or component identification and overview;

- Identification of business or organizational stakeholders and users;
- Definition of operational or functional capability requirements;
- Derivation of lower level functional capability requirements;
- Definition of non-functional requirements;
- Derivation of lower level non-functional requirements;
- Identification of requirements interdependencies;
- Identification of design constraints;
- Identification of product or component specific Quality Criteria;
- Identification of Data requirements.

In the analysis and formulation of requirements, requirements statements are produced in a structured way according to specific fields in tabular form. This supports consistency, readability and proper importing of requirements tables into the PANOPTESEC system engineering repository. The following fields must be used in the requirements table structure:

1. **id:** A unique identifier, that must be used for traceability and management of the requirement across the PANOPTESEC project;
2. **Description:** A plaintext description of the requirement. This description must make use of a key word in capital letters used to express the requirement with a formulation that is as unambiguous and as precise as possible. The allowed key words are defined below;
3. **Goal:** Used to express the objective of the function addressed by the defined requirement;
4. **MainPurpose:** Used to describe the justification of a corresponding function that would cover the requirement. It may give possible explanation concerning the context of the use of a function that addresses the requirement. Example(s) of the use of the function may be provided as a MainPurpose justification of the need fulfilled by the function.
5. **Importance:** The Importance value describes the importance of a requirement with respect to the stakeholder needs and provides a means to measure the success of the PANOPTESEC project. Importance is rated from 1 to 3. These three values are matched to the statements MAY (1), SHOULD (2) and MUST (3) key words in the Description field, where the key words are defined by RFC 2119 [1].
6. **Reachability:** The Reachability value describes the relative amount of research or development effort that is estimated to fulfill the requirements, rated from 1 to 3. A level 1 reachability rating requires integration of existing components; level 2 reachability rating requires specific development then integration, and level 3 reachability rating requires research, specific development and then integration.
7. **Version:** The Version provides a means to track changes to requirements and enables reference to compare past versions with current versions for traceability.

8. **Type:** Defines the kind of requirement, which can be “Functional” or “Non-Functional”.

The formulation of the ‘**Description**’ field must adhere to good practices for requirements statements including the following:

1. **Clear:** Consists of only a single requirement, easily read and understood by the stakeholders and avoids subjective or open-ended terms;
2. **Complete:** Contains sufficient detail to define the system or software function;
3. **Consistent:** Uses the same formulation structure and has no conflict with or duplication of other requirements;
4. **Uniquely identified:** Has a unique identification number;
5. **Unambiguous:** Must not be susceptible to multiple interpretations;
6. **Important or relevant:** Is either essential or desired to meet stakeholder objectives. The level of importance should be clear to the reader using defined terms [1];
7. **Reachable or appropriate to implement:** Is possible to achieve with an appropriate amount of effort even where that effort may require a combination of both advanced research and design or implementation activities;
8. **Verifiable (testable):** Stated in such a way that it is possible to evaluate if the requirement has been achieved by the implementation through inspection, analysis, test or demonstration;
9. **Free of implementation details:** Does not prescribe a particular approach to design or implementation.

To ensure the importance of a requirement is clear, the formulation of the ‘**Description**’ field must adhere to the following definitions in accordance with [1], wherein preference should be given to use of the key words “**MUS**T”, “**SHOULD**” and “**MAY**” (i.e., where possible, avoid the use of “**MUST NOT**” and “**SHOULD NOT**”):

- **MUST:** This word, or the terms "REQUIRED" or "SHALL", means that the definition is an absolute requirement of the specification.
- **MUST NOT:** This phrase, or the phrase "SHALL NOT", means that the definition is an absolute prohibition of the specification.
- **SHOULD:** This word, or the adjective "RECOMMENDED", mean that there may exist valid reasons in particular circumstances to ignore a particular item, but the full implications must be understood and carefully weighed before choosing a different course.
- **SHOULD NOT:** This phrase, or the phrase "NOT RECOMMENDED" mean that there may exist valid reasons in particular circumstances when the particular behavior is acceptable or even useful, but the full implications should be understood and the case carefully weighed before implementing any behavior described with this label.
- **MAY:** This word, or the adjective "OPTIONAL", means that an item is truly optional. One vendor may choose to include the item because a particular marketplace requires it or

because the vendor feels that it enhances the product while another vendor may omit the same item.

Importance is further defined by a numeric value in the '**Importance**' field from 1 to 3, according to the following scale:

- **MAY:** Represents 'Importance' value equal to '1';
- **SHOULD:** Represents 'Importance' value equal to '2'; and
- **MUST:** Represents 'Importance' value equal to '3'.

The '**Importance**' value will be used at the end of the project to assess the success of the PANOPTESEC project. It will also be used all along the project and especially at the end of each iteration to prioritize research and development: Priority should be given to level 3 (**MUST**) requirements, then to level 2 requirements (**SHOULD**), then to level 1 requirements (**MAY**).

The '**Reachability**' field describes a rough estimate of the level of effort needed to fulfill the requirement. It is rated from 1 to 3, according to the following scale:

- **Level 1:** Reachability requires integration of existing components;
- **Level 2:** Reachability requires specific component or sub-component development and integration;
- **Level 3:** Reachability requires research, specific component or sub-component development and then integration.

2.4 Requirements modeling

There are a variety of methods and mechanisms for modeling requirements in the domain of system and software engineering. The decision is based largely on the scope and complexity of the project, the skills and capabilities of the project team, and the familiarity or availability of specific tools.

In the case of the PANOPTESEC project, the requirements are modeled in SysML within the PANOPTESEC system engineering repository using the Eclipse-based Papyrus software [11]. Papyrus provides "an integrated and user-consumable environment for editing any kind of EMF model and particularly supporting UML and related modeling languages such as SysML and MARTE".

The PANOPTESEC system engineering repository is contained on a Subversion (SVN) server managed by the University of Lubeck (UoL).

It is the responsibility of the WP3 Leader to ensure requirements models are maintained within the PANOPTESEC system engineering repository. The WP3 Leader is supported by scientists and engineers from other WPs within the project.

2.5 Requirements traceability and coverage

Requirements traceability refers to the ability to trace the satisfaction of requirements from source, through derivation or refinement, into implementation, test and delivery. This traceability must be bi-directional. That is, the fulfillment of a preliminary objective, stated as a requirement should be traceable to the resulting verified feature or set of features within the system or software solution. Likewise a feature that is defined and verified within a system or software solution should be traceable to a source objective.

Requirements coverage refers to the degree of completeness that higher-level requirements have been satisfied by more detailed requirements or by system or software components or sub-components. Complete coverage is the ideal, wherein all requirements are completely covered by lower level requirements or system or software components. In practical terms, this is not always possible. However, it is important for coverage to be demonstrated within design files such that the impact of coverage that is less than 100% can be analyzed and the potential impact of missing coverage understood.

In the case of the PANOPTESEC project, the requirements traceability is managed in SysML using the Eclipse-based Papyrus software. The PANOPTESEC system engineering repository is contained on a Subversion (SVN) server managed by UoL.

It is the responsibility of the WP3 Leader to ensure requirements traceability is maintained within the PANOPTESEC system engineering repository. The WP3 Leader is supported by scientists and engineers from other WPs within the project.

2.6 Requirements validation

Requirements are validated with selected members of the stakeholder community to ensure resulting product will perform as per user intention in the identified environment. To ensure selected stakeholders understand and agree with the requirements, a Quality Review (QR) is conducted using the quality criteria established in the PANOPTESEC Peer Review Quality Assurance checklist [18], the PANOPTESEC Requirements Review Quality Assurance Checklist [19] and any additional quality criteria that may be established in the specific requirements document.

For an operational requirements document, an expert representative of the stakeholder community should lead the QR.

For a functional requirements document, the QR should be led by an expert of the operational stakeholder community provided the stakeholder representative has sufficient knowledge and understanding of software requirements analysis and formulation. Otherwise, the QR may be led by other scientists or engineers in the design team, not involved in the development of the specific requirements document undergoing review.

Depending on the type of requirement or stage within the iterative software development lifecycle (SDLC), it may be appropriate to provide demonstration of existing prototypes or mock-ups as part of the QR. Demonstrations can be a significant aid in ensuring the understanding of requirements. In this case the following may apply:

- Use of simulation models or storyboards; or
- Sample validation demonstration is created and shown to customer and records are maintained in the form of minutes of meeting (MOM).

Based on the review, any defects that are found in the requirements are recorded in the quality review summary report (QRSR), including appropriate actions for resolution.

Any contradictory requirements are discussed with the stakeholders and the Technical Project Manager (TPM). The TPM is responsible to identify and assess the risk (e.g., cost, schedule or resource impacts) related to requirements. The TPM is also responsible to inform the stakeholder concerning the risks, present a mitigation approach and come to a mutual agreement for risk treatment. Thus requirement analysis is done and balance is achieved.

Once all issues related to defects and contradictory requirements have been resolved, requirements are signed-off by stakeholders or domain experts as appropriate, thereby establishing the initial baseline of requirements.

2.7 Requirements management (including change control)

The Requirements Baseline (RB) represents a formal agreement between the selected stakeholder(s) and the project team. As a formal agreement, the RB must not be changed, except through mutual agreement by the stakeholder(s). Consequently, the RB is a Configuration Item (CI) and any change to the RB must follow the configuration management (CM) and change control (CC) process described in the PANOPTESC Configuration Management Plan 0.

2.8 Quality assurance

The QA in the PANOPTESEC project relies on the assessment of a work product (i.e. deliverable) according to lists of QA checks (QA checklists) [18] [19] established by a QAM, validated at a Consortium level and centralized in the Project Handbook [17].

For the purpose of the QA of the D2.2.1, the deliverable has been assessed according the following checklists:

- PEER REVIEW (PR) QA CHECKLIST [18]: the D2.2.1 deliverable is a report, it then requires a proper peer review according to the checks defined in this checklist;
- REQUIREMENTS REVIEW (RR) QA CHECKLIST [19]: the D2.1.1 deliverable being a Requirement document, it requires the assessment of the checks including in this checklist.

This QA validation process followed the Quality Review Procedure established by the QAM and was validated by the consortium. Detailed results of the review are captured in a report (called QRSR2.1.1). Checklists are available on the PANOPTESEC SVN.

3 THE PANOPTESEC SYSTEM

In this section, we present the PANOPTESEC system and its main functions.

3.1 Product perspective

As the dependency has grown on networks and computer systems, so too have the motives and capabilities of cyber adversaries to attack them. Regardless of their motives, cyber attackers are often able to penetrate networks and computer systems to extract valuable information (compromising confidentiality), tamper with the accuracy of the information (compromising integrity) and overload or otherwise prevent access to needed services and systems (compromising availability). Any of such tactics used by the cyber adversaries can have significant negative impacts on an organization's business, reputation and liabilities. In the era of open networks and platforms, pioneered by paradigms such as the internet, web services, cloud computing and mobile computing, attacks find more venues to exploit the complexity and scale of use to cause increasingly substantial damages.

The objective of the PANOPTESEC system is to be a beyond-state-of-the-art prototype of an automated cyber defence decision support system that is intentionally designed to meet FP7-ICT-2013-10 Objective ICT-2013.1.5 Trustworthy ICT item (c). That is, the PANOPTESEC consortium will deliver an operational prototype as a means to "prevent, detect, manage and react to cyber incidents in real-time, and to support breach notifications, improving the situational awareness and supporting the decision-making process" required by cyber operators. "It will also develop and demonstrate advanced technologies and tools that will empower users, notably individuals and SMEs, in handling security incidents".

3.2 Production functions

The PANOPTESEC system reaches its goals by implementing the following production functions:

- **Information collection from multiple data sources**: The PANOPTESEC system collects information about the monitored system by using generic and specific data collectors. Collected information deals with the monitored system steady state: network architecture, devices configuration, available services and their configuration, deployed security policy. They also deal with the dynamic events that happen in the system, such as system and network events as well as alerts raised by Intrusion Detection Systems (IDS). Finally, they also deal with security knowledge that is not specific to the monitored system such as vulnerability advisories.
- **Information correlation and abstraction**: The PANOPTESEC system correlates and abstracts collected information to generate relevant semantic-rich information that is used to feed the proactive and reactive responses systems. This semantic-rich information can also be displayed to the users of the PANOPTESEC system for them to understand the current situation in the monitored system.
- **Proactive response to reduce the steady-state risk level**: The PANOPTESEC system uses correlated and abstracted information to evaluate the steady-state risk level of

the monitored system(s) (i.e. the level of risk in the system while no attack is ongoing) and to reduce it by proposing and implementing modifications in the monitored system(s) configuration.

- **Reactive response to reduce the dynamic risk level**: The PANOPTESEC system uses correlated and abstracted information to evaluate the dynamic risk level of the monitored system(s) that, by contrast with the steady-state risk level, takes into account the attacks that are happening on the system (and that may have been detection by IDS). It also tries to reduce it by proposing and implementing modifications in the monitored system(s) configuration.
- **Visualization and user interactions**: The PANOPTESEC system provides a rich visualization and user interactions system that provides general situational awareness, helps the users in understanding the steady-state and dynamic risk levels and interacts with them to propose responses to be implemented to reduce them.

These high-level production functions are described with more details the PANOPTESEC Description of Work (DoW) [13]. They are also reflected in the High-Level Preliminary Design [10].

The PANOPTESEC system also has to answer to the objectives of FP7 ICT-2013-1.5 item c [14] that are summarized in Table 2.

id	Description	Version	Importance	Reachability
FP001	The resulting solution SHOULD aid Security Operators to prevent cyber-incidents in real-time	1	2	2
FP002	The resulting solution SHOULD aid Security Operators to detect cyber-incidents in real-time	1	2	2
FP003	The resulting solution SHOULD aid Security Operators to manage cyber-incidents in real-time	1	2	2
FP004	The resulting solution SHOULD aid Security Operators to react to cyber incidents in real-time	1	2	2
FP005	The resulting solution SHOULD provide breach notifications.	1	2	2
FP006	The resulting solution SHOULD improve situational awareness for Security Operators	1	2	2
FP007	The resulting solution SHOULD aid the Security Operators decision making process	1	2	2
FP008	The project SHOULD develop advanced technologies and tools	1	2	2

FP009	The project SHOULD demonstrate advanced technologies and tools	1	2	2
FP010	The project SHOULD empower Security Operators in handling security incidents, including SMEs.	1	2	2

Table 2: FP7-ICT-2013-1.5 item c Objectives.

Table 3Table 3 summarizes the objectives that were defined in the PANOPTESEC DoW [13].

id	Description	Version	Importance	Reachability
DOW001	The PANOPTESEC System MUST proactively calculate risk, identify and actuate courses of action based on evaluated operational impact due to updated knowledge of cyber vulnerabilities and changes in network and computer system configuration.	1	3	3
DOW002	The PANOPTESEC System MUST provide multi-sensor data integration and correlation of infrastructure, security and operation data through the use of advanced ontology and inference technologies.	1	3	3
DOW003	The PANOPTESEC System MUST reactively calculate risk, identify and enable Security Operators to actuate courses of action, based on evaluated operational impacts due to detected cyber incidents.	1	3	3
DOW004	The PANOPTESEC System MUST recommend to Security Operators reactive courses of action optimized to maximally deny attacker capabilities while minimizing operational impact.	1	3	3
DOW005	The PANOPTESEC System MUST provide the option to actuate reactive courses of action in a fully automatic mode (i.e., without operator intervention).	1	3	3
DOW006	The PANOPTESEC System MUST provide optimized notification of detected cyber incidents through the use of advanced technologies for multi-sensor data integration and	1	3	3

	correlation.			
DOW007	The PANOPTESEC System SHOULD provide an advanced visual analytics engine to improve Security Operator's ability to access and analyze large complex data sets.	1	3	3
DOW008	The PANOPTESEC System MUST provide proactive and reactive risk and response models resulting in optimized course of action recommendations to Security Operators.	1	3	3
DOW009	The PANOPTESEC project SHOULD deliver an integrated system of beyond-state-of-the-art security algorithms and software modules providing continuous monitoring and automated response for cyber defense.	1	3	3
DOW010	The PANOPTESEC project MUST conduct demonstrations on an operational segment of user agency (ACEA) for comparison of PANOPTESEC-delivered capabilities against the status quo.	1	3	3
DOW011	The PANOPTESEC project MUST deliver an integrated system for cyber security detection and response scalable for use by both SMEs and larger enterprises.	1	3	3

Table 3 : Objectives of the PANOPTESEC Project as Stated in the DoW.

The PANOPTESEC requirements have been elicited using these objectives.

3.3 Refining the objectives

During the first plenary meeting held on January 2014 in the Acea SpA premises in Rome, the consortium team had the first real chance to openly discuss with all the relevant people about the requirements for the project. It was pinpointed that, even if the Acea Group had clearly some very special requirements due to its custom technical configurations and layered offering in multiple areas, the PANOPTESEC consortium had to find a common ground usable for other user agencies too. Following this path, we exploited the experiences

of Acea SpA (particularly the work done to successfully handle previous IT security incidents and all the relevant information needed to do that on time) and the ISO 27001 / 27002 guidelines to underline the more general IT requirements trying to match them to the SCADA-specific ones. We even made comparisons with commercially available solutions and products with similar objectives (e.g. software tools like Skybox Security, technologies like Security Intelligence platforms). After an analysis of all information and ideas gathered, the consortium team compiled a list of items to be individually checked by the user agency panel (one expert for each interested area of the Acea Group): a lot of feedback was given to the consortium, to be discussed in multiple conference calls later. After some corrections and modifications (i.e. merging similar requirements to a less specific one, normalizing technical terms, etc.), a complete and workable list of items was then resubmitted to the SCADA/ICT technical experts of Acea SpA and finally to the whole consortium for the approval.

4 STAKEHOLDERS IDENTIFICATION

In the methodology (see section 2.1), four stakeholder categories have been identified: *client stakeholders, market stakeholders, partner stakeholders and user stakeholders*. In this section, we present the stakeholders that have been identified by the PANOPTESEC consortium for the PANOPTESEC system for each of these categories.

4.1 Client stakeholders

As mentioned earlier, client stakeholders represent those organizations or agencies for which there is a contractual relationship. In the case of the PANOPTESEC project, the client stakeholder is the European Commission. As the consequence, the PANOPTESEC system must comply with the selection criteria and objectives of the FP7 ICT-2013-1.5 item c [14] call as well as with the commitments that were made in the PANOPTESEC Description of Work [13]. Along the whole project, the PANOPTESEC consortium must also comply with the feedback provided during review meetings.

4.2 Market stakeholders

As stated earlier, market stakeholders represent the various market segments wherein the resulting product, system or software may be sold. Since the PANOPTESEC system can be used for both ICT systems and SCADA systems, the PANOPTESEC consortium has identified mid to large-sized corporations, as well as public institutions, that use one of these two kinds of systems, or both, as market stakeholders.

ACEA manages both ICT and SCADA systems. It is therefore a very important source of input about market stakeholders concerns. To avoid being too ACEA-specific, the PANOPTESEC consortium also benefits from inputs from the EAB (that comprises representatives of the European Defense Agency, of the French Information Systems Security Agency -*Agence Nationale de la Sécurité des Systèmes d'Information, ANSSI*-, of ABN-AMRO -*Algemene Bank Nederland-Amsterdam Rotterdam*, Banking sector-, of Infrabel -Public Transportation Sector-, of the Bulgarian Defense Institute and of the Royal Military Academy of Belgium) to better understand specific concerns of multiple relevant sectors (namely: defense, national

security, banking, energy and transportation) encompassing ICT and SCADA. Their feedback will be used to ensure that the PANOPTESEC system addresses the security needs of the market.

4.3 Partner stakeholders

As states earlier, partner stakeholders represent the participant organizations represented by the delivery team, namely ACEA S.p.A., Alcatel-Lucent Bell Labs France, Università Degli Studi Di Roma La Sapienza, Epistematica SRL, Institut Mines-Telecom, RHEA System S.A., Ecole Supérieure D'Électricité and Universität zu Lübeck. Partners influence the PANOPTESE project due to particular plans for research direction and outcomes, development plans or technology solutions, personnel development and training, as well as, eventual exploitation plans.

More precisely, partner stakeholders can be subdivided in the following profiles:

- **Technical Project Manager**: This partner stakeholder manages the technical work between the other Partners involved in the various Work Packages. He propose processes that ensure the smooth running of the technical progress, validates the produced results according to the global objectives of the Project as described in the DoW [13] to ensure technical high quality and consistency, and enforces the technical processes and the technical schedule of the project according to the DoW [13]. RHEA is the Technical Project Manager partner stakeholder for the PANOPTESEC project.
- **Project Coordinator**: This partner stakeholder coordinates all the aspects of the work between the other Partners involved in the Project, propose processes that ensure the smooth running of the Project within the Consortium and outside the Consortium, validate the produced results according to the global objectives of the Project as described in the DoW [13] to ensure high quality, consistency and pertinence, and enforces the processes and the schedule of the project according to the DoW [13]. IMT is the Technical Project Manager partner stakeholder for the PANOPTESEC project.
- **Work Package Leaders**: These partner stakeholders coordinate the work between the other Partners involved within a Work Package, validate the produced results according to the technical objectives of the Work Package as described in the DoW [13]. Their goal is to ensure high technical quality, and to enforce the schedule of their Work Package according to the DoW [13].
- **Deliverable Editors**: These partner stakeholders organize and coordinate the writing of deliverables between the other partners within a Work Package, validate the contributions to ensure the technical high quality of the deliverable, and enforce the schedule to respect the due date of the deliverable according to the DoW [13].
- **User Partner**: This partner stakeholder provides to other partners the operational context and requirements (e.g. use cases, scenarios, experimental dataset and test bed) and controls the appropriateness of the solution proposed by Solution

Providers to this operational context and requirements. It also tests the software architecture designed the IT Architect and developed by the Software Developers based on realistic cases. ACEA is the User Partner for the PANOPTESEC project.

- **Solution Providers**: These partner stakeholders propose scientific or technical solutions for which they are is skilled and recognized in their community, to fulfill one or several of the objectives of the sub-system (e.g. Dynamic Risk Management Response System, Visualization, etc.) researched, designed and developed in the purview of each Work Package. Being able to develop new concepts and tools as well as testing them is very important for PANOPTESEC solution providers.
- **IT Architect**: This partner stakeholder is interested in the quality, stability and performance of the PANOPTESEC overall architecture. Particularly, he is responsible of choosing and organizing the Integration Framework that will bind the various components of the PANOPTESEC system together. Therefore, efficient integration of the various components is very important for him.
- **Software Developers:** These partner stakeholders are interest in the quality, reliability, adequacy and performance of the various components of the system. Since their main focus is on each component, they need to rely on the Integration Framework for integration with the other components. Being able to use adequate and efficient programming languages and IDE is also very important for them.

4.4 User stakeholders

User stakeholders provide to other Partners the operational context and requirements (e.g. use cases, scenarios, experiment dataset and test bed) and control the appropriateness of the solution proposed by Solution Providers to this operational context and requirements. They may already be included as stakeholders already identified as Client, Market and/or Partner stakeholders. However, user stakeholders are more tightly coupled to the specific development activities and drive user interface and feature requirements. In the PANOPTESEC project, ACEA is at the same time a user stakeholder and a partner stakeholder. However, the PANOPTESEC consortium also considers other types of user stakeholders that operate into other relevant sectors such as defense, national security, banking, energy and transportation. To that end, the PANOPTESEC consortium benefits from inputs and feedback from the External Review Board which members are representative of these sectors.

More precisely, user stakeholders can be subdivided in the user profiles which characteristics are described in the next section.

5 ACTORS AND USER CHARACTERISTICS

In this section, we present the characteristics of the user stakeholders of the PANOPTESEC system. To that end, we first describe a high-level description of the users in the PANOPTESEC partner/user stakeholder, ACEA. The purpose of this description is not to reduce the scope of the PANOPTESEC system to this specific user stakeholder, but to

provide an illustrative example. Then, we present the user roles that have been identified. These user roles are specific enough to be used in requirements elicitation while generic enough to address the various sectors envisioned for the PANOPTESEC system (defense, national security, banking, energy and transportation).

The Acea Group operates in the water sector (integrated water cycle), in electricity chain, in public lighting and in gas. It has a strong local presence in and around Rome and some important alliances aimed to achieve the critical mass needed to maximize its efficiency and competitiveness throughout Italy. Due to the specific focus on SCADA systems, both for clean / waste water and electricity distribution, the user stakeholders have been identified in the control rooms of that specific sub-companies taking care of these services (Acea ATO2 for water, and Acea Distribuzione for electricity), in the ICT Security Operation Center room and in the Cyber Security Governance area (namely, "Sicurezza e Tutela"). The latter two, both part of the Acea SpA holding, are mentioned as user stakeholders as both previously cited sub-companies actually use services offered from these parties and must share part of their objectives and security-related information with them. Moreover, due to its specific role in the group security governance, the "Sicurezza e Tutela" people took the lead of the PANOPTESEC project for the Acea Group team.

Acea ATO2 SpA controls the SOA (acronym for "Sala Operativa Ambientale", that stands for "Environmental Control Room"), and serves more than 3,5MLN people taking care of the whole integrated water cycle.

Acea Distribuzione SpA controls the SOE (acronym for "Sala Operativa Elettrica", that stands for "Electricity Distribution Control Room") and is the only authorized distribution operator for Rome and its surroundings, serving more than 1,6MLN PODs (acronym of "Point of Delivery", most of them being actually smart meters).

The following **user roles** have been identified:

- **Business Owner/Manager:** A person with an executive level function within the organization interested in understanding the security status of the business (mission) processes and possible business impact due to cyber-attacks. He or she is also interested in improving the security level of the business he or she owns/manages for it to better fulfill its missions.
- **Monitored Systems Administrator**: A person who, for an organization, is responsible for the inventory, deployment or/and configuration management of hardware and software systems that compose the monitored system(s) on a day to day basis, with the focus to keep the monitored system(s) running and fulfilling their missions. These stakeholders provide input data related to the infrastructure, its configuration and on the kind of information that is useful for them to perform their tasks. Monitored System Administrators of SCADA systems are **Monitored SCADA Systems Administrators** (which is sub-role) and Monitored System Administrators of ICT systems are **Monitored ICT Systems Administrators** (which is sub-role). Monitored System Administrators that are actively involved with security (i.e. they use and configure security devices and services) are **Monitored System Security**

Administrators (which is sub-role). They provide information related to the Company Security Policies. Their focus is of keeping the monitored system secure according to the rules defined in a security policy. In some instances, Monitored Systems Administrators will have to be specifically involved to implement the chosen mitigation action (e.g., implementation of patches or making changes to the system configuration). In some organizations, Monitored Systems Administrator can be referred to as **Network Administrators**, **Network Operators**, **System Operators**, etc.

- **PANOPTESEC System Manager:** A person involved in setup and configuration of the data sensors interface with the PANOPTESEC system as well as any pre-configuration or configuration changes needed by the PANOPTESEC system (e.g., input the list of pre-approved mitigation actions). His focus is on keeping the PANOPTESEC up and running securely and in being able to make it evolve when necessary.
- **PANOPTESEC Security Operators:** Persons that are the primary users of the PANOPTESEC system. Operators have both proactive and reactive responsibilities. Proactive functions include reviewing vulnerabilities within the monitored system, reviewing potential mission impact, reviewing and selecting of mitigation actions and their execution. Reactive functions include reviewing indications of suspected cyber attacks, reviewing potential mission impacts, reviewing and selecting of mitigation actions and approval of execution.

All these user roles are educated persons that are supposed to be willing to actively perform their tasks. Specifically, it is supposed that the Business Owner/Manager has important knowledge of the business missions. It is also supposed that Monitored Systems Administrators are technically skilled about the systems they manage. They may however not be security-aware if they are not Monitored System Security Administrators. The PANOPTESEC System Manager is technically skilled but might not have as extensive security skills as PANOPTESEC Security Operators. PANOPTESEC Security Operators are technically skilled, especially about security. They understand the business missions, the global architecture of the monitored system and the link between the business missions and the architecture.

Aside these user roles that are real persons, the following actors have been identified:

- **Monitored System(s)**: This actor includes SCADA systems (e.g., database and/or SCADA servers, Front End Gateways, etc.) and ICT systems (e.g., Network devices, database servers, Domain Name Servers, computers used to access the infrastructure to perform operational roles, etc.). It is an information source for the PANOPTESEC system that collects numerous pieces of information about its configuration. It also receives mitigations actions from the PANOPTESEC system for deployment.
- **Cyber Sensors:** This actor corresponds to the sources of cyber relevant data (such as configuration scanners, IDS and log generators) within the Monitored System used by PANOPTESEC for security analysis and mitigation action planning and execution.

Finally, the PANOPTESEC system being a security solution, the **Threat Agent Actors (**also called **Attackers**) have to be considered. An attacker is a person, system or entity that performs advert actions on the ICT system of an organization that bypass the security policy in order to gain unauthorized information or privileges with the focus of harming the business or prevent the organization from achieving one or several of its missions. The role of the PANOPTESEC system is to counter these objectives. In more details, Threat Agent Actors can be:

- **Corporations:** In a competitive business environment adversaries may use cyber tools to acquire new market shares from others (may use Cyber spies, Cybercriminals or bribe employees).
- **Cyber Vandals:** These attackers derive thrills from intrusion or destruction of cyber property, without agenda (e.g. web site defacers).
- **Cyber warriors:** These attackers, with high skills and significant resources, may be able to cause major disruption on local/regional/national scale.
- **Cyber spies:** These attackers, that act individually or in small groups, may be hired from competitors or other parties, possessing high cyber skills and access to significant resources.
- **Cybercriminals:** These attackers may act individually or on behalf of others (e.g. mobsters and organized crime, business competitors) and uses their medium/high level cyber skills to attack / destroy cyber assets, abuse or steal resources. They act only for profit.
- **Cyber-terrorists:** These attackers are terrorists who rely on the use of cyber methods to support a specific socio-political agenda. They may be alone or organized in small groups, act on order or on opportunity targets (e.g. Al Qaeda, ISIS).
- **Employees:** current or former employee/operator of the system.
- **Hacktivists:** These attackers are highly motivated activists with cyber skills. They may eventually act in an organized crew or party, depending on role and personal capabilities (e.g. Anonymous).
- **Mobsters:** These attackers are managers of organized crime organization with significant resources.
- **Nation-states:** These attackers encompass various sovereign territories with significant resources to cause harm (may support Cyber-terrorists or use Cyber warriors or even Cybercriminals).

Given the numerous sectors the PANOPTESEC system can be applied to, all these Threat Agent Actors have to be considered. Table 4 provides more details about some of these threats agents by presenting their capabilities and tools. Figure 2 presents a scale of the threats due to the various threat agents.

	Threat Agents					
	Corporations	Cybercriminals	Employees	Hacktivists	Nation states	Terrorists
Drive-by exploits		✓				✓
Worms/Trojans		✓			✓	✓
Code Injection		✓		✓		✓
Exploit kits		✓				
Botnets	✓	✓		✓		✓
Denial of service		✓		✓	✓	✓
Phishing attacks		✓				
Compromising confidential information	✓	✓	✓	✓	✓	✓
Rogueware / Scareware		✓			✓	
Spam	✓	✓				
Targeted attacks	✓	✓			✓	✓
Physical Theft / Loss / Damage	✓	✓	✓		✓	✓
Identity theft	✓	✓	✓		✓	
Abuse of Information Leakage	✓	✓	✓	✓	✓	✓
Search Engine Poisoning	✓	✓				
Rogue certificates		✓			✓	

Table 4: Threat Agents / typical threats, capabilities and tools [15]

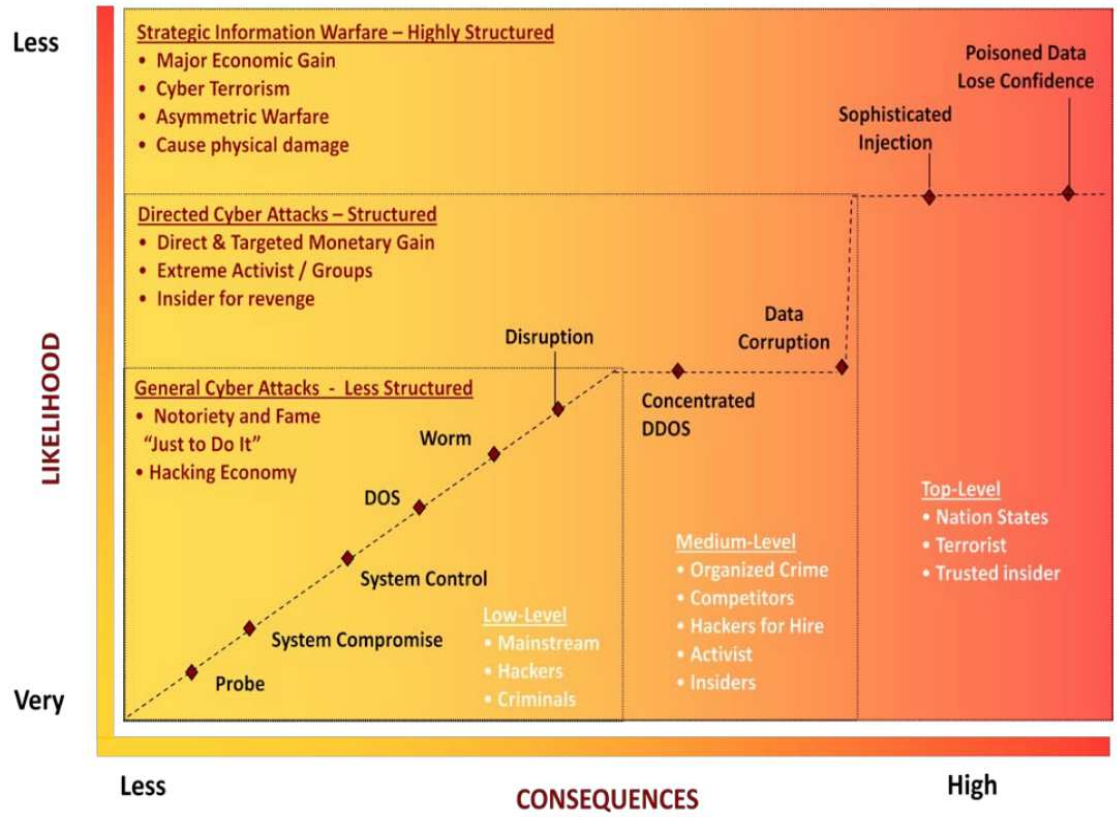

Figure 2: Graphical representation of the risk and threats/threat agents

6 USER SCENARIOS

In order to better understand the contexts of use of the PANOPTESEC system and describe actors' interactions, three user scenarios have been designed using [Scenario Template]. Aside a unique ID, a list of authors and a full text description, the template is organized to provide the following pieces of information:

- What are the objectives of the scenario? What aspect of the PANOPTESEC system use does it describe?
- Does the scenario illustrate the proactive response system of PANOPTESEC, the reactive response system of PANOPTESEC, or both?
- What business functions does the scenario model?
- Which are the actors (person, non-person and threat agents entities) that are involved in the scenario?
- What are the assumptions necessary for the scenario to happen? What are the system state and/or conditions that must be met before the scenario will execute? What is the system state after the described sequence of event has successfully executed?

- What would have been the normal flow of events if no security compromise had happened?
- What is the compromise that took place in the scenario?
- What are the expected frequency of occurrence and the probability of success?
- What is the impact of the compromise? What is the loss expectancy? What are the legal, personal, physical consequences of the compromise presented in the scenario?
- What is the flow of events and resulting business impact due to the compromise?
- What information would sensors generate that indicate that the compromise has taken place? What information would the PANOPTESEC system display to security operators that indicate that the compromise has taken place?
- What would be the valid and invalid mitigation options?
- What is the flow of events during the activation of the mitigation actions?
- It this scenario a priority? Is it related to another scenario?

These numerous items provide valuable information for all the partners and stakeholders. Especially, they describe how each of the high-level PANOPTESEC components should behave: What information should be collected and correlated, what proactive and reactive responses should be proposed and implemented, and what information should be displayed to the security operators.

Three main user scenarios have been created using this template. The first user scenario, UserScenario01 (cf. ANNEX A), describes attacks against command and control networks. The second user scenario, UserScenario02 (cf. ANNEX B), describes attacks against SCADA equipment/devices of a critical infrastructure performed through its SCADA command and control network. Finally, the third user scenario, UserScenario03 (cf. ANNEX C), describes attacks to one or more nodes that operate some IT services underlying a non-core business process.

In the following subsections, we briefly present these three user scenarios.

6.1 Attacks to the C&C systems of a Critical Infrastructure

The **objective** of UserScenario01 is to show the typical criticalities caused by the unavailability, loss of serviceability or subversion of a Command and Control center caused by cyber attacks targeting known vulnerabilities. Command and Control (C&C) centers and dedicated networks are used to manage SCADA devices and networks that are operating all Critical Infrastructures. The full version of this user scenario is available in ANNEX A: User Scenario 1, Attacks to Command and Control networks and systems of a Critical Infrastructure.

In the **normal flow of events**, the SCADA Operators perform regular operations to manage the Critical Infrastructure using the C&C system that connects to the SCADA devices in the

field. All the automated safeguards and balancing actions are working normally and are available. Overall, the systems are operating normally.

Dealing with PANOPTESEC operations, a MAPE (Monitor, Analyze, Plan, and Execute) process is followed. PANOPTESEC Security Operators *monitor* the system by reviewing the security status of the monitored system (SCADA and ICT environment). They *analyze* the security status indicators that may note the presence of one or more system vulnerabilities due to known software security flaws as posted by openly available vulnerability advisory services. Attack paths from hypothetical attack sources (both internal and external) to known mission critical systems are analyzed and the impact on critical business functions (e.g., energy distribution) is assessed resulting in a quantified risk assessment. During the *Plan* phase, prioritized mitigation actions are presented to the PANOPTESEC Security Operators that may consist of one or more discrete actions that collectively improve the steady-state risk level of the Monitored System (e.g., patch deployment or other system reconfiguration). Mitigation actions are selected and *executed* by the PANOPTESEC Security Operators resulting in automated deployment of mitigation actions where possible (e.g., firewall reconfigurations) or otherwise issuing instructions to Network, SCADA and ICT Operators for follow-up deployment of mitigations (e.g., patch deployment). Network, SCADA and ICT Operators receive notifications of mitigation actions from the PANOPTESEC Security Operators and take appropriate steps to implement the requested security mitigation actions. PANOPTESEC Security Operators also provide periodic status reports to Business Owners concerning the security status of their business (mission) operations. Business Owners provide oversight to Network, SCADA and ICT system operations.

The **compromise** happens when one or more threat agents exploit one or more vulnerabilities or use legitimate access rights to penetrate into, or to or otherwise attack one or more assets used for C&C of the Critical Infrastructure, such as:

- Compromise a gateway of SCADA commands flow.
- Compromise a server of SCADA commands.
- Compromise data flow to gain arbitrary view/control.
- Compromise an unspecific host in C&C network as botnet Zombie host.

Due to these actions, the C&C systems are either:

- Unable to reach / send SCADA commands to a large number of RTUs/PLCs and thus cannot perform regular operations to manage the targeted Critical Infrastructure devices; or
- Controlled by the cyber threat agents allowing them to execute arbitrary functions

If the C&C center is unable to properly manage the SCADA network it is responsible for, the Critical Infrastructure will continue to operate using previously programmed rules or scripted conditional actions stored inside the SCADA servers locally present in some sub-sites. This situation is normal due to possible connection problems and outages always present in large and geographically dispersed SCADA installations. However, the range of

acceptability for this condition varies depending on the real world situation, both in term of timing, number, criticality of unreachable nodes and/or missing pieces of SCADA information. Without any means for the C&C center to act on these unreachable nodes, or check their status, the operators will call for repairs while relying on the built-in resilience of the SCADA system itself. Possibly, operator personnel could receive notifications of service failures from field-based personnel, police or customers (e.g. phone calls, emails, support requests). In the worst case, should the C&C center lose the capability to manage the SCADA network and devices due to cyber attackers taking control of SCADA servers/devices, the attackers could cause critical damage to the infrastructure devices and cause catastrophic disruption of services delivery.

The **frequency of occurrence of this scenario** is low, but the **likelihood of success** is high. The **loss expectancy** (based specifically on ACEA's figures) is more than tens of thousands of Euros per minute.

Therefore, **business impact** encompasses complete or partial loss of control of the Critical Infrastructure due to the disruption of its Command and Control network capabilities, direct, indirect or collateral damage to the Critical Infrastructure itself, loss of awareness of the ongoing status of the Critical Infrastructure, loss of capability to support maintenance operations, and loss of capability to control or guarantee the core business services (e.g. electricity/water distribution). **Consequences** are legal exposure, economic loss, reputation loss, regulation compliance loss and potentially massive social impact.

For this scenario to happen, it is of course necessary that the Command and Control center is operative. The threat agent user also needs to access to public or private WAN networks that the monitored system owner uses. The PANOPTESEC system is operative and acquires information concerning the Monitored Systems. Supporting data is provided by non-monitored system references (e.g. public vulnerability databases).

This scenario encompasses continuous security monitoring capabilities operating in **both a proactive and reactive model**. Proactive security response improves the steady-state risk level of the monitored system. Reactive security response reacts to cyber attacks that may hinder or prevent the ability to control and remotely manage the Critical Infrastructure.

The **detection indicators** are the fact that the C&C center loses established network connections or can't accept/establish new connections to RTUs of the Critical Infrastructure. Security alerts are logged by security software/devices (e.g., firewall logs, intrusion detection system alerts, etc.) and PANOPTESEC system correlates them to on-going attacks.

The PANOPTESEC system should display as **analysis indicators** the possible attack paths to support PANOPTESEC Security Operators in understanding if the actual situation is similar to an attack to the C&C network of the Critical Infrastructure. Depending on the situation, **valid mitigation actions** may include, among others patch deployment, system update, port and protocol reconfigurations, routing reconfigurations, services shut down. However, **invalid** (proactive or reactive) **mitigation** options normally include any major blocking action on the network, any action that would disrupt the SCADA system in an uncontrolled manner.

After the application of the mitigation actions (**post condition**), the SCADA Operators regain control: all the previously affected systems are restored to proper operation and continue to maintain traces and audit logs.

6.2 Attacks to SCADA equipment/devices of a Critical Infrastructure

The objective of this scenario is to show the typical criticalities caused by the unavailability, loss of serviceability or subversion of the networks and systems comprising a Command and Control center caused by cyber attacks targeting known vulnerabilities of the SCADA equipment/devices of a Critical Infrastructure, performed through its SCADA Command and Control network.

Like in the previous scenario, in the **normal flow of event**, the SCADA Operators perform regular operations to manage the Critical Infrastructure using the C&C system that connects to the SCADA devices in the field. All the automated safeguards and balancing actions are working normally and are available. Overall, the systems are operating normally. Like in the previous scenario, a MAPE process is followed by the PANOPTESEC Security Operators.

The **compromise** happens when one or more threat agents exploit one or more vulnerabilities or use legitimate access rights to penetrate into assets of the Critical Infrastructure, example being:

- Compromise a gateway of SCADA remote unit in the field.
- Compromise SCADA Remote Unit to perform arbitrary command (not sent or showed from C&C system).
- Compromise SCADA Remote Unit flow (or Gateways) to put a “men in the middle” host/gateway.

Due to these actions, an attacker could perform:

- Command Action on critical infrastructure equipment with relative social impact.
- Send false data to the C&C system about real status of critical infrastructure equipment.
- Generate the “domino effect failure” (especially for electrical infrastructures) starting from one compromise Remote Unit.

If one or more attacks complete successfully, the attacker can gain and/or escalate privileges, compromise other assets or blocks the communications between the C&C center and the Critical Infrastructure devices (RTUs/PLC). After a successful compromise, the C&C center could therefore not be able to manage a significant part of the SCADA devices of the Critical Infrastructure. In the worst case, the SCADA devices of the Critical Infrastructure are not under (exclusive) control of the C&C center. They act differently compared to the original programming and pre-sets. Some compromised SCADA servers may be used to execute arbitrary functions and commands on the SCADA devices in the field.

The **frequency of occurrence of this scenario** is low, but the **likelihood of success** is high. The **loss expectancy** (based specifically on ACEA's figures) is more that tens of thousands of Euros per minute.

Business impact encompasses complete or partial loss of control of the Critical Infrastructure due to the disruption of its devices, direct damage to the Critical Infrastructure devices, loss of awareness of the ongoing status of the Critical Infrastructure, loss of capability to support maintenance operations, loss of capability to control or guarantee the core business services. Consequences are legal exposure, economic loss, reputation loss, regulation compliance loss and massive social impact.

For this scenario to happen the Command & Control system must be operating and threat agents have access to the external networks (only outer attack surface). The PANOPTESEC system is operative and acquires information concerning the Monitored Systems in the field. Supporting data is provided by non-monitored system references (e.g. public vulnerability databases).

This scenario encompasses continuous security monitoring capabilities operating in **both a proactive and reactive model**.

The **detection indicators** are based on the fact that the C&C center loses established network connections or can't accept/establish new connections to RTUs of the Critical Infrastructure. Security alerts are logged by security software/devices (e.g., firewall logs, intrusion detection system alerts, etc.) and the PANOPTESEC system correlates them to on-going attacks.

The PANOPTESEC system should display as analysis indicators the possible attack paths to support PANOPTESEC Security Operators to understand if the actual situation is similar to an attack to the Critical Infrastructure devices. Depending on the situation, **valid mitigation actions** may include among others patch deployment, system update, port and protocol reconfigurations, routing reconfigurations and/or ACL enabling or forcing RTU device in the field to use a different type of connection. However, **invalid** (proactive or reactive) mitigation actions would consist in blocking ALL SCADA commands, including legitimate ones or isolate RTU from network node vector attack path if possible.

After the application of the mitigation actions (**post condition**), the SCADA Operators regain control: all the previously affected systems are restored to proper operation and continue to maintain traces and audit logs.

6.3 Attack to nodes that operates some ICT services underlying a business process

The **objective** of this third scenario is to show the typical criticalities caused by the disruption of a business process due to unavailability, loss of serviceability or subversion of the underlying ICT services and devices, eventually applying proactive or reactive mitigation actions until the underlying ICT services and the business process are fully restored.

In the **normal flow of events**, the ICT systems are operating normally. If minor problems are present they are normal technical issues. A MAPE process is followed by the PANOPTESEC Security Operators

The **compromise** happens when one or more threat agents exploit one or more vulnerabilities or use legitimate access rights to penetrate into, or to otherwise attack one or more ICT assets used in support of business functions. Due to these actions, the ICT Services are either unable to reach / send / perform regular operation from IT services by related operator or controlled by the cyber threat agents allowing them to execute arbitrary functions.

After this, one or more threat agents could manage to reach the Core ICT Infrastructure network using one or more attack vectors / types (e.g. sending exploits to servers and communication devices, using DoS to silence the servers, use buffer overflows to subvert server services exposed, use fishing or spear fishing, etc.). If one or more attacks complete successfully, the attacker possibly gains even more privileges or get a hold on other reachable assets. After a successful compromise, the attacked IT devices could not operate the IT service any more or could operate normal IT service and other not required.

The **frequency of occurrence of this scenario** is low, and the **likelihood of success** is medium. The **loss expectancy** should be low but depends on the attacked IT service, its importance and the duration of the attack.

The **business impact** consists in the complete or partial loss of delivery of the attacked business function due to malfunction of some business processes and/or underlying sub-processes or devices (e.g. web servers of file servers). **Consequences are** legal exposure, economic loss, reputation loss and regulation compliance loss.

For this scenario to happen, the business process must first be operating normally. Threat agents have access to the network used from the IT service. They can access to public or private WAN networks that the user agency is actually using or access to the internal and/or external networks (e.g. ICT network, DMZ network) servicing the business process. The PANOPTESEC system is operative and acquires information concerning the Monitored Systems. Supporting data is provided by non-monitored system references (e.g. public vulnerability databases).

This scenario encompasses continuous security monitoring capabilities operating in **both a proactive and reactive model**.

Detection indicators consist in security alerts that are logged by security software/devices (e.g., firewall logs, intrusion detection system alerts, anti-virus logs, connection logs, etc.). The PANOPTESEC system should correlate them to on-going attacks. The PANOPTESEC system should present the possible attack paths to support PANOPTESEC Security Operators in understanding if the actual situation is similar to an attack to the IT Service. **Valid mitigation actions include** anti-virus launch, patch deployment, system update, port and protocol reconfigurations, routing reconfigurations and/or ACL enabling/modifying, device quarantine. **Invalid mitigation options** depend on the attacked service and the nature of its nodes/devices.

After the application of the mitigation actions (**post condition**), the Network and ICT Operators regain control: all the previously affected systems are restored to proper operation and continue to maintain traces and audit logs.

7 FUNCTIONAL REQUIREMENTS

In this section, we present the functional operational that have been elicited for the PANOPTESEC system. For clarity purposes, these functional operational requirements are grouped according to the high-level preliminary design [10] component they belong to:

- Data Sources and Collection (DSC);
- Information Correlation and Abstraction (ICA);
- Proactive Response System (PRS);
- Reactive Response System (RRS);
- Visualization (VIZ).

All the requirements proposed in the following subsections are *functional*. The **Functional/Non Functional** column has been removed due to space constraints.

7.1 Operational Requirements for Data Sources and Collection

Operational Requirements for Data Sources and Collection are related to the data sources that are used by the PANOPTESEC system and to the collection process. Their unique id begins with DSC.

id	Description	Goal	MainPurpose	Importance	Reachability	Version
DSC001	The PANOPTESEC system MUST provide a data collection system	Ensuring that the PANOPTESEC system uses data that are representative of the current state of the system and of threats.	In order to perform proactive and reactive response, data about the system and threats are necessary.	3	1	1
DSC002	The data collection system MUST provide a standard based interface for data collection from data sources forming part of the monitored system(s).	Ensuring an as automated as possible mechanism to collect data to reduce the burden of collecting data.	Collecting data manually is an error-prone human resource-consuming task. Automated collection of data through standard based interfaces both reduces human resources impact and limits errors.	3	2	1

DSC003	The data collection system MUST provide a standard based interface for data collection from the data sources not forming part of the monitored system(s) (e.g., vulnerability advisory sources).	Ensuring that data that are not specific to the monitored systems (vulnerability advisories for instance) are also automatically collected.	The PANOPTESEC system uses not only information from the monitored system (i.e. IDS/IPS/FWS logs), but also public vulnerability advisory databases (CVE). As standard based-interfaces exist, it would be inefficient and error prone not to benefit from them.	3	2	1
DSC004	The data collection system MUST provide non-standard interfaces (i.e. proprietary) for data collection from data sources that have non-standard data interfaces.	Ensuring that the PANOPTESEC takes advantage of relevant data sources even if no standard interface is available.	Some very useful tools export results in proprietary formats only. The PANOPTESEC system MUST nevertheless be able to benefit from them.	3	3	2
DSC005	The data collection system SHOULD store all raw data received by the PANOPTESEC system from the monitored and non-monitored system(s).	Ensuring that no piece of data is lost during the process and that an analyst can benefit from every piece of data that was collected.	Very small details coming from raw data can sometimes be very useful to an analyst. As a consequence, the PANOPTESEC system SHOULD store every piece of information that was collected, for instance for forensics purpose.	2	2	2

DSC006	The data collection system MUST collect system configuration information.	Ensuring that the proactive and reactive response systems perform computations on valid monitored system configurations.	Threats and alerts are to be considered very differently according to the fact that they target a system that exhibits the corresponding vulnerability or not. Having actual system configuration information helps in evaluating threats and alerts.	3	1	1
DSC007	The system configuration information MUST contain information about the ICT devices of the monitored system(s).	Ensuring that the PANOPTESEC system is suited for monitored systems that are made of ICT devices.	ICT devices and networks are the most common types of information systems. The PANOPTESEC system must therefore address their needs.	3	1	1
DSC008	The ICT system configuration information MUST contain information about the operating systems running on the ICT devices.	Ensuring that the proactive and reactive response system benefits from the knowledge about the operating system each device runs to evaluate threats and alerts.	Threats and alerts have to be evaluated according to the operating systems running on the machines. A threat or alert related to a given vulnerability in a given OS should for instance be minimized if the detected target does not use this OS/version.	3	1	1

DSC009	The ICT system configuration information MAY contain information about the device drivers installed on the ICT devices (signed, unsigned, WHQL, experimental, unknown source, and others if available).	Ensuring that the proactive and reactive response system benefit from the knowledge about the drivers that are installed on the monitored ICT systems.	Drivers are pieces of software that have extensive privileges on the device they run on. They are therefore a target of choice for attackers and should be particularly taken care of when evaluating threats and alerts.	1	2	2
DSC010	The ICT system configuration information MAY contain information about the root certificates installed on the ICT devices (SSL/TLS);	Ensuring that the PANOPTESEC can benefit from knowledge about the root SSL/TLS certificates that are installed on the ICT devices.	Root SSL/TLS certificates are used by web browsers to decide if a given entity with which they communicate is legitimate. They are for instance used to authenticate web servers or software update servers. Attackers often compromise the root SSL/TLS certificate repository of the devices they have compromised.	1	1	2

DSC011	The ICT system configuration information MUST contain information about the firmware installed on the ICT devices.	Ensuring that the PANOPTESEC system also handles ICT devices other than computers. Routers, printers and firewalls should for instance be taken into account.	Non-PC devices such as routers and printers are nowadays a target of choice for attackers because their security is often overlooked. New vulnerabilities are often discovered against them and patches must be applied. Therefore, the PANOPTESEC system MUST take firmware versions into account when analyzing threats and alerts.	3	2	1
DSC012	The ICT system configuration information MUST contain information about the software applications running on the ICT devices.	Ensuring that the proactive and reactive response system benefit from the knowledge about the applications that are installed on the monitored ICT system.	Applications vulnerabilities are often targeted by attackers to enter a system or to elevate their privileges. Therefore, the PANOPTESEC system MUST take applications and their versions into account when analyzing threats and alerts.	3	2	2

DSC013	The ICT system configuration information MUST contain device identification information including MAC Address, IP Address, ICT device names and other device tags or unique serial numbers if available (i.e., IMEI for phones).	Ensuring that the proactive and reactive response system benefit from the knowledge about the network configuration of the devices that are part of the monitored ICT system.	Nowadays, Information systems are intensively networked and most of attacks/malware use this medium to propagate. The PANOPTESEC system must therefore take this aspect into account and maintain knowledge about network configuration of the ICT system.	3	2	1
DSC014	The ICT system configuration information MUST contain information about the layer 3 network topology.	Ensuring that the proactive and reactive response system benefit from the knowledge about the network topology of the monitored ICT system.	The network topology is a very important information for instance to decide on the reachability of a given device from another. The PANOPTESEC system must therefore take this information into account and maintain information about the layer 3 (IP) network topology.	3	2	2

DSC015	The ICT system configuration MUST contain information about both human and machine users and their permissions.	Ensuring that the proactive and reactive response system benefit from the knowledge about the security policy that should be enforced in the monitored ICT system, and especially users rights, users being human or machine.	The security policy is very important information to decide if an action that has been performed is malicious. In fact, a malicious action is sometimes defined as an action that violates the security policy.	3	2	2
DSC016	The ICT system configuration information about users and their permissions MAY include permissions for file system access.	Ensuring that the proactive and reactive response system benefit from the knowledge about the file permissions.	File permissions (read, write and execute for instance) are very important information w.r.t. security policy enforcement for data confidentiality, integrity and availability.	1	2	2
DSC017	The data collection system MUST collect security policy information.	Ensuring that the proactive and reactive response system benefit from the knowledge about the security policy that should be enforced in the monitored ICT system.	The security policy is very important information to decide if an action that has been performed is malicious. In fact, a malicious action is sometimes defined as an action that violates the security policy.	3	2	1

DSC018	The system configuration information MUST contain information about the Supervisory Control and Data Acquisition (SCADA) devices on the monitored system(s).	Ensuring that the PANOPTESEC system is suited for monitored systems that are made of SCADA devices.	SCADA systems are envisioned to be a major target for cyber-attackers. The PANOPTESEC system therefore needs to address them.	3	2	1
DSC019	The SCADA system configuration information MUST contain information about the software applications running on the SCADA devices.	Ensuring that the proactive and reactive response system benefit from the knowledge about the applications that are installed on the monitored SCADA devices.	Applications vulnerabilities are often targeted by attackers to enter a system or to elevate their privileges. Therefore, the PANOPTESEC system MUST take applications and their versions into account when analyzing threats and alerts. This is particularly true for applications running on SCADA systems that have the reputation to often be particularly insecure.	3	3	1

DSC020	The SCADA system configuration information MUST contain information about the multiple instances of firmware running on the SCADA devices.	Ensuring that the proactive and reactive response system benefit from the knowledge about the applications that are installed on the monitored SCADA devices.	SCADA systems often rely more on firmware than on full OS. Multiple firmware versions can run on a given system. Since some vulnerabilities are firmware versions specific, it is important that the PANOPTESEC proactive and reactive response system take this information into account.	3	3	1
DSC021	The SCADA system configuration information MUST contain device identification information about the SCADA devices including serial numbers, device tags, location identifiers, and others if available.	Ensuring that the PANOPTESEC system can identify each SCADA device in the monitored systems and its properties.	To provide useful results, the PANOPTESEC system must be able to provide useful information about the SCADA devices in the monitored system.	3	2	1
DSC022	Security policy management MUST support complex organizational structures including multiple partners, affiliates or	Ensuring that the PANOPTESEC system can handle realistic structures that comprise more than one security authorities.	Medium to large companies often are made of various affiliate or subsidiaries that are submitted to different authorities from an information system security	3	2	1

	subsidiaries, each having different security authorities.		perspective. The PANOPTESEC system MUST address this aspect.			
DSC023	The data collection system MUST collect information describing the operational (or business) missions supported by the monitored system(s).	Ensuring that the proactive and reactive response system benefit from the knowledge about the operational and business mission supported by the monitored system(s).	Having information about the parts of the monitored system that are critical to the mission is very important when computing the risks against the mission, the potential remediation actions and for rating the potential remediation actions.	3	1	1
DSC024	The operation (or business) mission information MAY be automatically collected from system configuration information.	Ensuring an as automated as possible mechanism to collect operation or business mission information to reduce the burden of collecting data.	Collecting data manually is an error-prone human resource-consuming task. Automated collection of data both reduces human resources impact and limits errors.	1	3	1

DSC025	It MUST be possible to collect operation (or business) mission information from operator input.	Ensuring that the PANOPTESEC system takes advantage of relevant operation (or business) mission information even if it is not possible to collect them automatically.	A lot of operation (or business) mission information may not be collected automatically. However, the PANOPTESEC system must benefit from them and therefore must propose a way to collect them manually.	3	3	2
DSC026	The data collection system MUST collect information forming a pre-configured list of authorized operator mitigation actions.	Ensuring that the PANOPTESEC system will be able to propose some mitigation actions to the operator when necessary.	It is important that the PANOPTESEC system is able to propose in a timely manner some authorized mitigation actions. Having this pre-configured list ensures that some mitigation actions can be proposed and reduces the analysis and reaction time.	3	3	2

DSC027	It MUST be possible for the list of authorized operator mitigation actions to be collected from manual input	Ensuring that the list of authorized operator mitigation action will always be populated, even if no automatic collection mechanism is proposed or suitable.	The operators' expertise and knowledge on their system is a decisive advantage. They are the most knowledgeable people about the monitored system and how to reduce compromise in its specific context. The PANOPTESEC system will benefit from this fact by authorizing manual collection of authorized operator mitigation actions.	3	3	2
DSC028	The data collection system MUST collect information from at least one of the most well-known vulnerability advisory databases (e.g., National Vulnerability Database, Bugtraq, etc.) including at least one from Europe and one from the USA.	Ensuring that the PANOPTESEC system will have an as up-to-date as possible knowledge of the currently known vulnerabilities to compute risks and mitigation actions.	New vulnerabilities are made public everyday. The PANOPTESEC system MUST use the freshest information about currently know vulnerabilities to detect and mitigate attacks that would target recent vulnerabilities.	3	1	2

DSC029	The data collection system MUST collect network and system events (e.g., cyber security alerts from intrusion detection systems).	Ensuring that events (e.g. IDS alerts) in the system are available and taken into account by the PANOPTESEC reactive response system.	Host-based and Network-based IDS alerts are real-time information about the monitored system(s) and the attacks against it (them). The PANOPTESEC system must take benefit from them to have an as up-to-date as possible knowledge of its (their) current state.	3	1	1
DSC030	The data collection system MUST collect information about the deployed sensors and IDSes and their configuration.	Ensuring that the event (e.g. IDS alerts) can be verified and enriched according to information about the deployed sensors and IDSes and their configuration.	As sensors and IDSes sometimes generate incomplete or false alarms (false-positive for instance), it is important to have information about the deployed sensors and their configuration to reduce the number of false-positive alerts.	3	1	2

DSC031	The data collection system MUST collect information about devices physical location.	Ensuring that the PANOPTESEC system can inform operators about the physical location of each ICT device in the monitored systems in case an on-site operation has to be performed on it.	In large systems that can be spread over many different sites, it is important to be able to inform operators about the location of the various devices so as to reduce mitigation action time when on site operations have to be performed.	3	1	2
DSC032	The ICT system configuration information SHOULD contain information about the layer 2 network topology.	Ensuring that information about MAC layer configuration can be used by the PANOPTESEC system to compute risks and mitigation actions.	Some attacks, especially against SCADA systems, are performed at the MAC layer. Having information about layer 2 network topology is therefore important to detect these attacks and propose relevant mitigation actions.	2	2	1
DSC033	The ICT system configuration information MAY contain information about the layer 1 network topology.	Ensuring that information about Physical layer configuration can be used by the PANOPTESEC system to compute risks and mitigation actions.	Some attacks are performed against the Physical layer (Wi-Fi eavesdropping of signal jamming for instance). Having information about layer 1 network topology is therefore useful to detect these attacks and propose relevant mitigation actions.	1	2	1

Table 5: Operational Requirements for Data Collection and Correlation

7.2 Operational Requirements for Information Correlation and Abstraction

Operational Requirements for Information Correlation and Abstraction are related to data processing that is performed on collected data such as low-level correlation. Their unique id begins with ICA.

id	Description	Goal	MainPurpose	Importance	Reachability	Version
ICA001	The PANOPTESEC system MUST contain an information correlation engine.	Ensuring that the PANOPTESEC system can correlate automatically the various collected and computed pieces of information.	Since the PANOPTESEC system collects very different types of information from many sources, it is fundamental to provide an engine that is capable of correlating the various pieces of information automatically.	3	1	1

ICA002	The information correlation engine SHOULD translate multisource information received by the data collection system into a semantic (logic-based) common information representation.	Ensuring that the internal representation of the information in the PANOPTESEC system is consistent whatever the format (syntax) of the data when it was acquired.	The PANOPTESEC system will collect pieces of information from various sources. For a given kind of input (IDS alerts for instance), different sources may provide data in different formats. For efficient correlation, a common semantic representation must be defined to which pieces of data collected in different formats can be translated.	2	3	2
ICA003	The information correlation engine MUST identify common information elements across the multi-source information received by the data collection system.	Ensuring that the PANOPTESEC system has a common internal data model to handle consistently the pieces of information coming from various sources.	The various data sources used by the PANOPTESEC system may have different representations and syntaxes to describe what is actually the very same concept (semantically equivalent). The PANOPTESEC system internal data model MUST be able to define when two syntactically different pieces of data refer to the same concepts from a semantic perspective.	3	3	1

ICA004	The information correlation engine MUST resolve conflicts between information elements across the multi-source information received by the data collection system.	Ensuring that the PANOPTESEC system can handle conflicting pieces of information coming from various data sources.	Some pieces of information coming from various data sources may be conflicting, given for instance the fact that these data sources do not have the same access to the monitored system. The PANOPTESEC system MUST be able to resolve these conflicts.	3	3	1
ICA005	The information correlation engine MUST create a unified view of the monitored system from the multi-source information received by the data collection system.	Ensure that the PANOPTESEC system offers to the users a consistent representation of the information gathered from the various data sources.	As many very different sources of information are used by the PANOPTESEC system, it is mandatory that information is displayed in a unified way so as to be understandable, especially by security operators.	3	3	1
ICA006	The information correlation engine MUST store all information correlation results in the PANOPTESEC system.	Ensure that information correlation results are persistent.	It is very important to know, even after a long time, what was the state of the system and on what basis decisions have been taken. It can for instance be useful in the context of forensics of Advanced Persistent Threats (APT), or for compliance.	3	2	1

ICA010	The PANOPTESEC system MUST include a mission impact model.	Ensure that mission impact is taken into account by the PANOPTESEC system.	Taking into account the Mission Impact allows to better analyze the current state of the system and to propose more adequate responses. It is an important differentiator of the PANOPTESEC system by comparison with existing SIEM solutions.	3	2	1
ICA011	The mission impact model MUST describe relevant aspects of the mission (or business) operations supported by the monitored system(s) (e.g., mission, business process, tasks and activities).	Ensure that the relevant aspects of the mission (or business) operations are taken into account by the Mission Impact model of the PANOPTESEC system.	Mission impact models can take into account the mission in itself, the business process, tasks and activities. These various aspects must be taken into account by the PANOPTESEC system.	3	3	1

ICA012	The mission impact model MUST describe the dependencies between the mission (or business) operations and the software applications running on ICT devices of the monitored system(s).	Ensure that the dependencies are taken into account and clearly expressed between the mission and the ICT devices/applications that take part in the monitored system.	To be useful in the context of the PANOPTESEC project, the mission impact model must not be conceptually disconnected from the software applications running on the ICT devices of the monitored system.	3	3	1
ICA013	The mission impact model MUST describe the dependencies between the mission (or business) operations and the software applications running on SCADA devices of the monitored system(s).	Ensure that the dependencies are taken into account and clearly expressed between the mission and the applications on SCADA devices that take part in the monitored system.	To be useful in the context of the PANOPTESEC project, the mission impact model must not be conceptually disconnected from the software applications running on the SCADA devices of the monitored system.	3	3	1

ICA014	The mission impact model MUST describe the dependencies between the mission (or business) operations and the multiple instances of firmware running on SCADA devices of the monitored system(s).	Ensure that the dependencies are taken into account and clearly expressed between the mission and the multiple instances of firmware on the SCADA devices that take part in the monitored system.	To be useful in the context of the PANOPTESEC project, the mission impact model must not be conceptually disconnected from the multiple firmware on the SCADA devices that are part of the monitored system.	3	3	1
ICA015	The mission impact model MUST be able to identify mission critical systems supporting the mission (or business operations).	Ensure that mission critical systems are identified by the mission impact model.	Mission critical systems are part of the monitored system that have to be protected in priority. The mission impact model MUST be able to identify them.	3	3	1
ICA016	The identified mission critical systems MUST encompass mission critical software applications running on ICT devices supporting the mission (or business operations).	Ensure that mission critical software applications running on ICT devices are identified by the mission impact model.	Mission critical systems are part of the monitored system that has to be protected in priority. The mission impact model MUST be able to identify them.	3	3	1

ICA017	The identified mission critical systems MUST encompass mission critical software applications running on SCADA devices supporting the mission (or business operations).	Ensure that mission critical software applications running on SCADA devices are identified by the mission impact model.	Mission critical systems are part of the monitored system that have to be protected in priority. The mission impact model MUST be able to identify them.	3	3	1
ICA018	The identified mission critical systems MUST encompass the multiple instances of mission critical firmware running on SCADA devices supporting the mission (or business operations).	Ensure that mission critical instances of firmware running on SCADA devices are identified by the mission impact model.	Mission critical systems are part of the monitored system that has to be protected in priority. The mission impact model MUST be able to identify them.	3	3	1
ICA019	The mission impact model MUST describe the mission impact due to cyber security compromise of identified mission critical systems.	Ensure that mission impact of cyber security compromise of mission critical systems can be assessed.	It is very important to be able to assess the consequences on the mission of mission critical system to understand the extent of a successful attack and to evaluate the efficiency of the proposed responses.	3	3	1

ICA020	The mission impact model MUST describe the mission impact due to mitigation actions contained in the preconfigured list of approved operator mitigation actions.	Ensure that the mission impact of mitigation actions can be assessed.	It is very important to be able to assess the impact of mitigation actions to be able to filter and prioritize them.	3	3	1

Table 6: Operational Requirements for Information correlation and abstraction

7.3 Operational Requirements for the Proactive Response System

Operational Requirements for the Proactive Response System are related to the way the PANOPTESEC system evaluates and improves the steady-stated security level of the monitored system (i.e., without taking events and alerts into consideration). Their unique id begins with PRS.

id	Description	Goal	MainPurpose	Importance	Reachability	Version
PRS001	The PANOPTESEC system MUST provide a proactive response system.	Ensure that the PANOPTESEC system can propose proactive responses to improve security of the monitored system(s).	The PANOPTESEC system must be able to propose proactive responses to improve the security of the monitored system even when no attack is performed.	3	1	1

PRS002	The proactive response system MUST evaluate the potential cyber security attack paths present in the system.	Ensure that attack path in the monitored system are evaluated.	Potential cyber security attack paths describe the various paths an attacker could follow in the monitored system. These paths must be identified and evaluated by the PANOPTESEC system.	3	1	1
PRS003	The proactive response system MUST evaluate the potential cyber security attack paths from hypothetical attack sources to identified mission critical systems.	Ensure that the attack paths evaluated by the PANOPTESEC system takes into account the identified mission critical systems as well as hypothetical attack sources.	Mission critical systems are a target of choice. Therefore, it is important that attack paths leading to them are carefully considered by the PANOPTESEC system.	3	3	1
PRS004	The evaluation of potential cyber security attack paths by the proactive response system MUST take into account system configuration information.	Ensure that attack paths evaluation takes into account the system configuration of the devices on the path.	As attack paths evaluation considers vulnerabilities of the devices/applications that are on a given path, and as vulnerabilities can depend of the configuration of devices and application, attack paths evaluation MUST take into account system configuration information.	3	2	1

PRS005	The evaluation of potential cyber security attack paths by the proactive response system MUST take into account security policy information.	Ensure that attack path evaluation takes into account the system configuration of the devices on the path.	The implemented security policy can have important consequences on the security of a device/application. Therefore, attack paths evaluation MUST take into account system security policy information.	3	3	1
PRS006	The evaluation of potential cyber security attack paths by the proactive response system MUST take into account current vulnerability advisory information.	Ensure that vulnerability advisories are taken into account during attack path evaluation.	Vulnerability advisories provide valuable information about devices/applications that are vulnerable, and for which software version. The fact that a device/piece of software is vulnerable has important consequences on the security of this device, and therefore on the attack path evaluation. Therefore, attack path evaluation must take vulnerability advisories into account.	3	2	1

PRS007	The proactive response system MUST evaluate the steady state level of risk based on the potential cyber security attack paths present in the system.	Ensure that the steady state level of risk of the monitored system(s) is evaluated based on potential attack paths.	The steady state level of risk of the monitored system(s) is a very valuable piece of information that defines what is the current status of this system from a security perspective and the accepted risks. The steady state level of risk is related to the risk level of the easiest attack path evaluated.	3	1	1
PRS008	The evaluation of steady state level of risk by the proactive response system MUST take into account current mission impact information.	Ensure that the steady state level of risk of the monitored system(s) is evaluated based on mission impact.	The impact of a successful attack depends heavily on the fact that the target of this attack is mission critical. This aspect should therefore be taken into account in the evaluation of the steady state level of monitored system(s).	3	3	1
PRS009	The proactive response system MUST evaluate the steady state level of risk independent from network and system events (i.e., excluding cyber security alerts from intrusion	Ensure that the evaluated steady state level of alert focuses on the steady state of the monitored system.	The steady state level of risk of the monitored system is a long-term indication that MUST only take into consideration the steady state of the system.	3	1	1

	detection systems).					
PRS010	The proactive response system MUST propose mitigation actions to maximally reduce the evaluated steady state level of risk to identified mission critical systems.	Ensure that the PANOPTESEC system proposes the most efficient mitigation actions to improve the security of the mission critical system.	Mitigation actions proposed by the PANOPTESEC proactive response system MUST improve the long term security of the monitored system(s) (and especially of mission critical systems), which consists in reducing the steady state level of risk.	3	1	1
PRS011	The mitigation actions proposed by the proactive response system MUST minimize the mission impact to identified mission critical systems.	Ensure that the PANOPTESEC system proposes the most efficient mitigation actions to minimize the mission impact to mission critical systems.	Mission critical systems are the most important part of the monitored system(s). To really improve security of the monitored systems, mitigation actions proposed by the PANOPTESEC proactive response system MUST therefore take into account minimizing impact of attacks on them.	3	3	1

PRS012	The mitigation actions proposed by the proactive response system MUST be derived from a pre-configured list of approved operator mitigation actions.	Ensure that the PANOPTESEC proactive response system can use a pre-configured list of actions to propose mitigation actions.	To automatically propose mitigation actions, the PANOPTESEC system needs a generic knowledge base that describes what kinds of actions can be taken to reduce each type of risks. This is the role of the pre-configured list of approved mitigation actions.	3	3	1
PRS013	The proactive response system MAY enable hypothetical evaluation of the steady state level of risk to identified mission critical systems through manipulation of system configuration information, vulnerability advisory information, network topology information, mission impact information and approved operator mitigation actions.	Ensure that the PANOPTESEC proactive response system may consider hypothetical configurations of the monitored system to propose mitigation actions.	In order to find mitigation actions that would reduce the steady state level of risk and/or the impact of potential attacks on mission critical systems, the PANOPTESEC proactive response system may evaluate the steady state level of risk/impact of attack on hypothetical system configurations and propose the mitigation actions that lead to these hypothetical states.	1	3	2
PRS014	The proactive response system MUST enable	Ensure that the security operator is given choices	Mitigation actions proposed by the PANOPTESEC proactive	3	3	1

	the operator to select proposed mitigation action for actuation.	about the mitigation actions to be deployed.	response system may be inadequate due to the fact that some contextual information was not available during computation. Therefore, the security operator MUST be able to select the proposed mitigation actions to be deployed.			
PRS015	The proactive response system MUST enable the operator to activate any selected mitigation action for actuation.	Ensure that the security operator can chose to deploy any of the mitigation actions that were proposed.	No mitigation action should be proposed that couldn't technically be deployed.	3	3	1
PRS016	The proactive response system MUST actuate (implement) mitigation actions activated by the operator for actuation.	Ensure that the selected mitigation actions are actually deployed.	For the security to be improved by the PANOPTESEC system, the selected mitigation action MUST be actually deployed.	3	2	1

PRS017	The actuation (implementation) of mitigation actions MUST be policy driven, based on contextual policies and suggest the activation of the optimal mitigation actions.	Ensure that the mitigation actions are deployed in accordance with the security policy.	Deployed mitigation actions MUST NOT conflict with the security policy. If adequate, they SHOULD even improve implementation of the security policy.	3	1	2
PRS022	The proactive response system MUST deploy the selected mitigation actions in the monitored system.	Ensure that the mitigation actions selected by the security operator are actually deployed.	For the security to be improved by the PANOPTESEC system, the selected mitigation action MUST be actually deployed.	3	3	2

Table 7: Operational Requirements for the Proactive Response System

7.4 Operational Requirements for the Reactive Response System

Operational Requirements for the Reactive Response System are related to the way the PANOPTESEC system evaluates and improves the dynamic security level of the monitored system. By contrast with the Proactive Response System, the Reactive Response System takes events and alerts into consideration. Operational Requirements for the Reactive Response System unique id begins with RRS.

id	Description	Goal	MainPurpose	Importance	Reachability	Version
RRS001	The PANOPTESEC system MUST provide a reactive response system.	Ensure that the PANOPTESEC can detect events and attacks in the monitored system(s) and react accordingly.	Events and attacks happening in the monitored system(s) MUST be detected and mitigation actions must me proposed and deployed to reduce risks.	3	1	1
RRS002	The reactive response system MUST evaluate the dynamic risk level to identified mission critical systems.	Ensure that the PANOPTESEC reactive response system evaluates the dynamic risk level to identified mission critical systems to be able to respond accordingly.	By contrast with the steady-state risk level, the dynamic risk level depends on events and alerts that are detected in the monitored system. The dynamic risk level therefore particularly depends on the ongoing attacks and must be evaluated.	3	3	1
RRS003	The reactive response system MUST evaluate the dynamic risk level based on network and system events (e.g., including cyber security alerts from intrusion detection systems).	Ensure that the PANOPTESEC reactive response system takes network and system events (including IDS alerts) into account to evaluate the dynamic risk level.	Network and hosts events and alerts are representative of what is currently happening on the monitored system. They MUST be taken into account when computing the dynamic risk level of the monitored system.	3	3	1

RRS004	The evaluation of dynamic risk level by the reactive response system MUST take into account system configuration information.	Ensure that system configuration is taken into account to evaluate the dynamic risk level.	System configuration has a big impact on the attack surface of the monitored system. It must therefore be taken into account to compute the dynamic risk level of the monitored system.	3	2	1
RRS005	The evaluation of dynamic risk level by the reactive response system MUST take into account security policy information.	Ensure that security policy is taken into account to evaluate the dynamic risk level.	Deployed security policy has a big impact on the attack surface of the monitored system. It must therefore be taken into account to compute the dynamic risk level of the monitored system.	3	3	1
RRS006	The evaluation of dynamic risk level by the reactive response system MUST take into account current vulnerability advisory information.	Ensure that vulnerability advisory information is taken into account to evaluate the dynamic risk level.	Vulnerability advisories provide valuable information about devices/applications that are vulnerable, and for which software version. Therefore, they have an impact on opportunities for attackers in the monitored systems. Vulnerability advisory information must	3	2	1

			therefore be used by the PANOPTESEC system to evaluate the dynamic risk level of the monitored system(s).			
RRS007	The reactive response system MUST evaluate the dynamic risk level based on the potential cyber security attack paths present in the system.	Ensure that potential cyber security attack paths present in the system are taken into account to evaluate the dynamic risk level.	The potential cyber security attack path evaluated by the PANOPTESEC proactive response system provides important pieces of information about the attack path that would most probably be used by an attacker. It is therefore a very precious source of information when computing the dynamic risk level.	3	3	1
RRS008	The evaluation of dynamic level of risk by the reactive response system MUST take into account current mission impact information.	Ensure that mission impact information is taken into account to evaluate the dynamic risk level.	Mission impact evaluation provides important pieces of information about the devices/application which compromise induces the biggest risk. It is therefore a very precious source of information when computing the dynamic risk	3	3	1

			level.			
RRS009	The reactive response system MUST propose mitigation actions to maximally reduce the evaluated dynamic level of risk to identified mission critical systems.	Ensure that the PANOPTESEC reactive response system proposes mitigation actions that efficiently reduce the evaluated dynamic level of risk to mission critical systems.	Mission critical systems are to be protected in priority. Mitigation actions proposed by the PANOPTESEC reactive response system MUST find a trade-off between risk reduction and impact minimization.	3	1	2
RRS010	The mitigation actions proposed by the reactive response system MUST minimize the mission impact to identified mission critical systems.	Ensure that the PANOPTESEC reactive response system proposes mitigation actions that efficiently minimize the mission impact to identified mission critical systems.	Mission critical systems are to be protected in priority. Mitigation actions proposed by the PANOPTESEC reactive response system MUST find a trade-off between risk reduction and impact minimization.	3	3	2

RRS011	The mitigation actions proposed by the reactive response system MUST be derived from a pre-configured list of approved operator mitigation actions.	Ensure that the PANOPTESEC reactive response system can use a pre-configured list of actions to propose mitigation actions.	To automatically propose mitigation actions, the PANOPTESEC system needs a generic knowledge base that describes what kinds of actions can be taken to reduce each type of risks. This is the role of the pre-configured list of approved mitigation actions.	3	3	1
RRS012	The reactive response system MAY enable hypothetical evaluation of the dynamic risk level through manipulation of system configuration information, vulnerability advisory information, network topology information, mission impact information and approved operator mitigation actions.	Ensure that the PANOPTESEC reactive response system may consider hypothetical configurations of the monitored system to propose mitigation actions.	In order to find mitigation actions that would reduce the dynamic level of risk and/or the impact of potential attacks on mission critical systems, the PANOPTESEC reactive response system may evaluate the dynamic risk/impact of attack on hypothetical system configurations and propose the mitigation actions that lead to these hypothetical states.	1	3	2

RRS013	The reactive response system MUST enable the operator to select proposed mitigation action for actuation.	Ensure that the security operator is given choices about the mitigation actions to be deployed.	Mitigation actions proposed by the PANOPTESEC reactive response system may be inadequate due to the fact that some contextual information was not available during computation. Therefore, the security operator MUST be able to select the proposed mitigation actions to be deployed.	3	3	2
RRS014	The reactive response system MUST enable the operator to activate any selected mitigation action for actuation.	Ensure that the security operator can chose to deploy any of the mitigation actions that were proposed.	No mitigation action should be proposed that couldn't technically be deployed.	3	3	2
RRS015	The reactive response system MUST actuate (implement) mitigation actions activated by the operator for actuation.	Ensure that the selected mitigation actions are actually deployed.	For the security to be improved by the PANOPTESEC system, the selected mitigation action MUST be actually deployed.	3	3	2

RRS016	The reactive response system MUST be able to model, compute and process multi-step attack scenarios based on topological and business information.	Ensure that multi-step attack scenarios are taken into account by the PANOPTESEC reactive response system.	In most cases, attackers will have to perform multiple attacks to reach their real goals. The PANOPTESEC reactive response system MUST therefore be able to model, compute and process multistep attack scenarios. To that end, it will use topological information (for reachability) and business information.	3	2	2
RRS017	The reactive response system MUST be fed automatically with complex correlation rules generated from attacks trees issued by the risk analysis phase.	Ensure that the PANOPTESEC reactive response system can benefit from complex correlation rules obtained from the risk analysis phase.	Correlation rules allow analyzing the various events and alerts that happen on the monitored network. They can be obtained from attack trees particularly. The PANOPTESEC reactive response system must use these correlations rules.	3	3	1

RRS018	The reactive response system MAY suggest the activation of mitigation actions based on contextual policies.	Ensure that contextual policies may be taken into account when proposing activation of mitigation actions.	Contextual policies provide refinement on what should be authorized or not on a system. The PANOPTESEC reactive response system may use contextual policies to take into account these refinements.	1	1	2
RRS023	The reactive response system SHOULD benefit from the use of anomaly detection, in order to derive new attack patterns.	Ensure that anomaly detection is taken into account by the PANOPTESEC reactive response system to derive new attack patterns.	Most of the IDS that are currently deployed today have a knowledge base of known attack that they can detect. Another way of detecting attacks is to have a knowledge base of normal device/application/user behavior and to detect deviations from these normal patterns, also called anomaly. Anomaly detection allows detecting new attack patterns and SHOULD be used in the PANOPTESEC reactive response system.	2	3	2

RSS024	The reactive response system MUST deploy the selected mitigation actions in the monitored system.	Ensure that the mitigation actions selected by the security operator are actually deployed.	For the security to be improved by the PANOPTESEC system, the selected mitigation action MUST be actually deployed.	3	3	1
RRS025	The reactive response system MUST be able to correlate alerts with multi-step attack models.	Ensure that multi-step attack models are used by the PANOPTESEC reactive response system to correlate alerts.	Multi-step attack models are generic high-level scenarios that can be used by an alert correlator to detect multi-step attacks based on the collected alerts. The PANOPTESEC reactive response system MUST use multi-step attack models to correlate alerts.	3	3	1
RRS026	The reactive response system MUST be able to automatically generate multi-step attack models and correlation rules.	Ensure that multi-step attack models and correlation rules are automatically generated by the reactive response system.	Multi-step attack models and correlation rules can be automatically generated and instantiated for a given specific system based on abstract multi-step attack models and correlation rules. The PANOPTESEC reactive response system MUST perform this task.	3	3	1

RRS027	The reactive response system SHOULD be able to tolerate uncertainty on the event data generated by the monitoring system (e.g., false alerts, missing alerts, etc.).	Ensure that the PANOPTESEC reactive response system can perform even when some of the malicious events are not detected or when legitimate events are erroneously detected as malicious.	One of the limitations of IDS is that they sometimes don't detect attacks (false negative) or sometimes erroneously report a legitimate event as an attack (false positive). The PANOPTESEC reactive response system SHOULD be able to tolerate IDS false positive and false negative when correlating alerts.	2	3	1

Table 8: Operational Requirements for the Reactive Response System

7.5 Operational Requirements for Visualization

Operational Requirements for Visualization are related to the way the PANOPTESEC system presents information and interact with users. Operational Requirements for Visualization unique id begins with VIZ.

id	Description	Goal	MainPurpose	Importance	Reachability	Version
VIZ001	The PANOPTESEC MUST provide a visualization system that displays cyber defense situational awareness in real-time.	Ensure that the PANOPTESEC system provides a real-time cyber defense situational awareness visualization system.	The PANOPTESEC real-time cyber defense situational awareness visualization system MUST allow security operators to understand the situation in the monitored system(s) and to interact with the PANOPTESEC	3	1	2

			system.			
VIZ002	The displayed cyber defense situational awareness MUST represent the steady state risk level to identified mission critical systems derived by the proactive response system.	Ensure that security operators know and understand the steady state risk level to identified mission critical systems.	At all time, security operators MUST be aware of the steady state risk level related to identify mission critical systems.	3	3	1
VIZ003	The displayed cyber defense situational awareness MUST represent the anticipated mission impact due to the steady state risk level to identified mission critical systems.	Ensure that security operators know and understand the anticipated mission impact due to the steady state risk level to identified mission critical systems.	At all time, security operators MUST know and understand what could happen in the identified mission critical systems given the current steady state risk level.	3	3	1
VIZ004	The displayed cyber defense situational awareness MUST represent the dynamic risk level to identified mission critical systems derived by the reactive response system.	Ensure that security operators know and understand the dynamic risk level to identified mission critical systems.	At all time, security operators MUST be aware of the dynamic risk level related to identified mission critical systems.	3	3	1

VIZ005	The displayed cyber defense situational awareness MUST represent the anticipated mission impact due to the dynamic level risk to identified mission critical systems.	Ensure that security operators know and understand the anticipated mission impact due to the dynamic risk level to identified mission critical systems.	At all time, security operators MUST know and understand what could happen in the identified mission critical systems given the current dynamic risk level.	3	3	1
VIZ006	The visualization system MUST enable the operator to display detailed information about identified mission critical systems information.	Ensure that details about identified mission critical systems can be displayed on demand.	Since the PANOPTESEC visualization systems MUST provide an overview of the current monitored system, it MUST also allow security operators to conceptually zoom on the monitored system and to obtain details on demand about identified mission critical systems.	3	3	2
VIZ007	The monitoring system MUST enable the operator to display detailed information about system configuration.	Ensure that details about system configuration can be displayed on demand.	Steady state and dynamic level of risk depend on system configuration. Therefore, the PANOPTESEC visualization system must allow security operators to obtain details on demand about system configuration.	3	2	2

VIZ008	The visualization system MUST enable the operator to display detailed information about Layer 3 network topology information.	Ensure that details about layer 3 (IP) network topology can be displayed on demand.	Steady state and dynamic level of risk depend on layer 3 (IP) network topology. Therefore, the PANOPTESEC visualization system must allow security operators to obtain details on demand about layer 3 (IP) network topology.	3	2	2
VIZ009	The visualization system MUST enable the operator to display detailed information about vulnerability advisory information from all sources used in the PANOPTESEC system.	Ensure that details about vulnerability advisories can be displayed on demand.	Steady state and dynamic level of risk depend on vulnerability advisories. Therefore, the PANOPTESEC visualization system must allow security operators to obtain details on demand about vulnerability advisories.	3	1	2
VIZ010	The visualization system MUST enable the operator to display detailed information about cyber security attack paths information.	Ensure that details about cyber security attack paths can be displayed on demand.	Steady state and dynamic level of risk depend on cyber security attack paths information. Therefore, the PANOPTESEC visualization system must allow security operators to obtain details on demand about cyber security attack paths	3	2	2

			information.			
VIZ011	The visualization system MUST enable the operator to display detailed information about network and system events (e.g., cyber security alerts) in real time.	Ensure that details about network and system events can be displayed on demand.	Dynamic level of risk depends on network and system events. Therefore, the PANOPTESEC visualization system must allow security operators to obtain details on demand about network and system events.	3	2	2
VIZ012	The visualization system MUST display the mitigation actions proposed by the proactive response system.	Ensure that mitigation actions proposed by the proactive response system are displayed by the PANOPTESEC visualization system.	The PANOPTESEC visualization system MUST display the current situation of the monitored system and the changes proposed by the proactive response system.	3	3	2
VIZ013	The visualization system MUST enable operator selection of mitigation actions proposed by the proactive response system.	Ensure that mitigation actions proposed by the proactive response system can be selected by security operators through the PANOPTESEC visualization system.	The PANOPTESEC visualization system MUST allow display of information and allow user interaction. Selection of mitigation actions is one of these interactions.	3	3	2

VIZ014	The visualization system MUST display the mitigation actions proposed by the reactive response system.	Ensure that mitigation actions proposed by the reactive response system are displayed by the PANOPTESEC visualization system.	The PANOPTESEC visualization system MUST display the current situation of the monitored system and display the changes proposed by the reactive response system.	3	3	2
VIZ015	The visualization system MUST enable operator selection of mitigation actions proposed by the reactive response system.	Ensure that mitigation actions proposed by the reactive response system can be selected by security operators through the PANOPTESEC visualization system.	The PANOPTESEC visualization system MUST allow display of information and allow user interaction. Selection of mitigation actions is one of these interactions.	3	3	2
VIZ016	The visualization system MUST enable operator activation of operator selected mitigation actions.	Ensure that security operators can activate mitigation actions using the PANOPTESEC visualization system.	The PANOPTESEC visualization system MUST allow display of information and allow user interaction. Activation of mitigation actions is one of these interactions.	3	2	2

VIZ017	The visualization system MAY enable operator input of mission impact information.	Ensure that mission impact information can be input by security operators using the PANOPTESEC visualization system.	Some pieces of mission impact information cannot be automatically collected. Therefore, security operators have to add them manually. Doing so through the PANOPTESEC visualization system make it more consistent since the PANOPTESEC visualization system becomes the single interaction point between security operators and the PANOPTESEC system.	1	3	2
VIZ018	The visualization system MUST enable the operator to designate systems as identified mission critical systems.	Ensure that information about mission critical systems can be input by security operators using the PANOPTESEC visualization system.	Information about what are the identified mission critical systems cannot be automatically collected. Therefore, security operators have to add it manually. Doing so through the PANOPTESEC visualization system make it more consistent since the PANOPTESEC visualization system becomes the single interaction point between	3	3	2

			security operators and the PANOPTESEC system.			
VIZ019	The visualization system MUST enable the operator to enter a mission impact description for security compromise to identified mission critical systems.	Ensure that mission impact description for security compromise to identified mission critical systems can be input by security operators using the PANOPTESEC visualization system.	Mission impact description for security compromise to identified mission critical systems cannot be automatically collected. Therefore, security operators have to add it manually. Allowing doing so through the PANOPTESEC visualization system makes it more consistent since the PANOPTESEC visualization system becomes the single interaction point between security operators and the PANOPTESEC system.	3	2	2
VIZ020	The visualization system MAY enable detailed display of raw information available in the PANOPTESEC system.	Ensure that detailed raw information available in the PANOPTESEC system can be displayed on demand.	Raw information available in the PANOPTESEC system may help security operators in understanding what is happening. Therefore, the PANOPTESEC visualization system must allow security operators to obtain details on demand about raw	1	2	2

			information available in the PANOPTESEC system.			
VIZ021	The visualization system MUST provide information about the actual system vulnerabilities	Ensure that actual system vulnerabilities can be displayed by the PANOPTESEC visualization system.	For security operators, Information about actual system vulnerabilities is very important to understand steady state and dynamic risk levels. Therefore, the PANOPTESEC visualization system MUST display them.	3	2	2
VIZ022	The visualization system representation of actual system vulnerabilities MUST differentiate between exploitable and non-exploitable vulnerabilities.	Ensure that exploitable and non-exploitable vulnerabilities are displayed differently by the PANOPTESEC visualization system.	As many vulnerabilities may exist in a medium-to-large sized monitored system, it would be counter-productive to display exploitable and non-exploitable one in the same manner. Indeed, it would overwhelm security operators and would make it much more complicated to understand what the risk is really due to. Therefore, exploitable and non-exploitable vulnerabilities must be displayed differently by the	3	1	2

			PANOPTESEC visualization system.			
VIZ023	The PANOPTESEC visualization system SHOULD enable historical data analysis.	Ensure that historical data can be displayed by the PANOPTESEC visualization system.	Analyzing historical data about the monitored system(s) can be really useful for security operators to better understand current situations. The PANOPTESEC visualization system SHOULD therefore display historical data on demand to allow historical data analysis.	2	3	2
VIZ024	The PANOPTESEC visualization system analysis of historical data SHOULD enable timeline based comparison of the status of the monitored systems (e.g., using snapshots or similar techniques).	Ensure that timeline-based comparisons of the status of the monitored system(s) are available in the PANOPTESEC visualization system to help security operators to perform historical data analysis.	Timeline-based comparison of the status of the monitored system is a common and efficient way to allow historical data analysis. The PANOPTESEC visualization system SHOULD propose it.	2	3	2

VIZ025	The visualization timeline comparison of the status of monitored systems SHOULD allow the operator to shift the analysis focal point forward and back in time while illustrating changes from one status to another.	Timeline-based comparison of the status of the monitored system is a common and efficient way to allow historical data analysis. The PANOPTESEC visualization system SHOULD propose it.	To allow efficient user interaction for historical data analysis using timeline-based comparison, security operators SHOULD be able to shift the analysis focal point forward and backward and see evolutions along time.	2	3	2
VIZ026	The visualization system MUST allow an operator to ask for stopping a reactive mitigation action to an ongoing attack.	Ensure that security operators can stop a reactive mitigation action.	Automatically deployed reactive mitigation actions could in fact be dangerous for the monitored system. Security operators MUST be able to stop such a reactive mitigation action using the PANOPTESEC visualization system.	3	3	2

VIZ027	The visualization system SHOULD provide the operator with representations to estimate the consequences of an ongoing attack	Ensure that security operators can access representations of the consequences of an ongoing attack to estimate them.	In limited time and while an attack is ongoing, it could be difficult for a security operator to fully understand the consequences of this attack. Therefore, the PANOPTESEC visualization system SHOULD provide security operators with representations to estimate the consequences of an ongoing attack.	2	3	1
VIZ028	The visualization system SHOULD provide the operator with mechanisms to easily share any information about the situation.	Ensure that security operators can easily share information about the situation.	Efficient communication between security operators is very important for them to perform and be reactive. Therefore, the PANOPTESEC visualization system SHOULD provide operators with mechanisms to easily share any information about the situation.	2	1	2

VIZ029	The visualization system SHOULD enable the operator to display detailed information about Layer 2 network topology information.	Ensure that security operators can access to detailed information about Layer 2 network topology.	Some attacks, especially against SCADA systems, are performed at layer 2 (MAC). Security operators SHOULD therefore benefit from representations about layer 2 (MAC) network topology proposed by the PANOPTESEC visualization system to understand precisely these attacks.	2	2	1
VIZ030	The visualization system MAY enable the operator to display detailed information about Layer 1 network topology information.	Ensure that security operators can access to detailed information about Layer 1 (Physical) network topology.	Some attacks are performed against the Physical layer (Wi-Fi eavesdropping of signal jamming for instance). Security operators SHOULD therefore benefit from representations about layer 1 (Physical) network topology proposed by the PANOPTESEC visualization system to understand precisely these attacks.	1	2	1

Table 9: Operational Requirements for Visualization

8 NON-FUNCTIONAL REQUIREMENTS

In this section, we present PANOPTESEC non-functional requirements. According to the ISO 25010:2011 standard [2], non-functional requirements have been elicited and grouped according to seven categories:

- Performance/Efficiency
- Compatibility
- Usability
- Reliability
- Security
- Maintainability
- Portability

All the requirements presented in the following subsections are *non-functional*. The **Functional/Non Functional** column has been removed due to space constraints.

8.1 Performance/Efficiency Requirements

Non-functional Performance/Efficiency Requirements are related to the *performance of the PANOPTESEC system relative to the amount of resources used under stated conditions* [2]. It encompasses time behavior, resource utilization and capacity. Non-functional Performance/Efficient Requirements unique id begins with PRF.

id	Description	Goal	MainPurpose	Importance	Reachability	Version
PRF001	The PANOPTESEC System SHOULD improve Security Operator course of action determination time from days to minutes in response to awareness of new cyber vulnerabilities and changes in network and computer system configuration.	Ensure that the PANOPTESEC system really improves the situational awareness of security operators.	Understanding precisely the state of the monitored system, the events that happen and what is to be done on it is a very difficult task as soon as the system is made of more than a few machines. The PANOPTESEC system intends to improve this situation.	2	3	1
PRF002	The PANOPTESEC system SHOULD reduce the total number of cyber incident alerts generated from multiple alert sensors (e.g., IDS, Firewalls, Syslog servers) by up to 25% through alert correlation functions.	Ensure reduce the number of false positive alerts that are provided to Security Operators and provide semantically rich real positive alerts.	Security Operators are often overwhelmed by false positive and/or semantically poor alerts. The PANOPTESEC system benefit from its correlation system to reduce false positive and improve the semantic value of the alerts it raises.	2	3	1

PRF003	The PANOPTESEC system SHOULD reduce the false negative cyber incident detection rate of a single Intrusion Detection System (IDS) by at least 25%, through alert correlation of multiple cyber incident detection sources.	Ensuring that the PANOPTESEC system detects more real malicious actions that a single Intrusion detection system.	The PANOPTESEC system will benefit from its multiple information sources and its correlation systems to improve the detection rate on real malicious action compared to a single intrusion detection system.	2	3	1

PRF004	The PANOPTESEC project SHOULD analyze system scalability using analytical methods to derive expected PANOPTESEC system response times in environments ranging from 10 to 10,000 nodes, in various typical network topologies (e.g., interconnected star and limited mesh) wherein nodes have a range from 1 to 10 applications installed and 10%, 20% and 30% of nodes each have a range of 1 to 3 vulnerabilities present.	Ensuring that the PANOPTESEC system can scale to monitor medium to large systems.	Systems made of hundreds of nodes are common and systems made of thousands of nodes can be found. The PANOPTESEC system SHOULD be designed to scale to networks of this size.	2	3	1

PRF005	The PANOPTESEC components SHOULD be able to each run in a 32GB dual core 2Ghz Virtual machine.	Ensure that the PANOPTESEC system can be used on common computers.	The PANOPTESEC system should not require exceptionally powerful server that would be too expensive. Also, the virtual servers used for the experimentation and demo phases must not be too expensive.	2	3	1
PRF006	The PANOPTESEC system SHOULD reduce Security Operator response time from hours to seconds in response to identified cyber incidents.	Ensure that the PANOPTESEC system reduces Security Operator response time.	When a security incident is detected, reaction time is paramount to reduce its impacts. The PANOPTESEC reactive response system must reduce this reaction time from hours to seconds.	2	3	1
PRF007	The PANOPTESEC System SHOULD reduce operator analysis of security status from days to minutes.	Ensure that the PANOPESEC system helps Security Operator understanding of the monitored system.	Understanding precisely the state of the monitored system and the events that happen on it is a very difficult task as soon as the system is made of more than a few machines. The PANOPTESEC system intends to improve this situation.	2	3	1

PRF008	The PANOPTESEC System MUST propose only approved course of actions responses that do not adversely affect operations.	Ensure that the PANOPTESEC system will not harm the monitored system.	Security Operators have to respond very fast to events. Furthermore, response is often performed under stress. The PANOPTESEC system MUST NOT propose responses that may adversely affect operations and may be selected erroneously by Security Operators.	3	2	1

Table 10: Performance and Efficiency Non-Functional Requirement

8.2 Compatibility Requirements

Non-functional Compatibility Requirements are related to the *degree to which* the PANOPTESEC system *can exchange information with other products, systems or components, and/or perform its required functions, while sharing the same hardware or software environment* [2]. It encompasses co-existence and interoperability. Non-functional Compatibility Requirements unique id begins with CMP.

id	Description	Goal	MainPurpose	Importance	Reachability	Version
CMP001	The PANOPTESEC System MUST be modular and decomposed in different components in order to improve flexibility (in	Ensure that each component can be modified/replaces with little impact on the other components.	The PANOPTESEC is made of various components that interact. While these components are closely related, it is important that modifications can occur in each of them with minimal	3	2	1

	organization and configuration), ability to develop new function combinations rapidly and component re-use		impact on the design and implementation of the others.			
CMP002	Communications between the various functional components of the PANOPTESEC System MUST be handled in a transparent way by a middleware in order to reduce complexity for developers.	Ensure that developers will not spend too much time handling network communications.	Network communications design, implementation and debugging can rapidly become complicated. Developers of the PANOPTESEC project MUST be able to focus on components functionalities and should not waste time on network communications.	3	2	1
CMP003	Functional components SHOULD access to collected data in a transparent way to reduce complexity for developers.	Ensure that developers will not spend too much time handling collected data access.	Data access design, implementation and debugging can rapidly become complicated. Developers of the PANOPTESEC project MUST be able to focus on components functionalities and should not waste time on collected data access.	2	2	1

CMP004	Communications between the various functional components of the PANOPTESEC System SHOULD allow the use of different patterns, both asynchronous and synchronous (e.g. Publish/Subscribe, Request/Reply, Point-to-Point and other Enterprise Integration)	Ensure that each component can benefit from the most suited communication pattern according to its needs.	The various components of the PANOPTESEC system have specific needs with respects to communication patterns. All these communication patterns must be available.	2	2	1
CMP005	The PANOPTESEC system MUST accept alerts in IDMEF format.	Ensure that IDMEF can be used as an input format for alerts.	IDMEF is currently the most common alert format. Many IDS technologies can generate alerts using this format. For maximum compatibility, this format must be accepted by the PANOPTESEC system.	3	1	1
CMP006	To cope with IDS that would not produce alerts in IDMEF, a translator to IDMEF SHOULD be provided.	Ensure that IDS that do not export alerts in IDMEF can still be used.	Some commonly used IDS export alerts only in proprietary format and not in IDMEF. A translator will be provided for all the IDS used as data source by the	2	2	1

			PANOPTESEC system that do not export natively in IDMEF to ease alert collection.			
CMP007	It SHOULD be possible to deploy the various functional components of the PANOPTESEC system on the same physical machine or on different machines.	Ensure that deployment of the various components of the PANOPTESEC system can be optimized according to the available hardware and to the size of the monitored system.	A deployed PANOPTESEC system must be able to evolve according to the monitored system. For some contexts, all components can be located on the same physical machine while for some others, different physical machines will be more appropriate.	2	1	1
CMP008	It SHOULD be possible for a system administrator to manage the runtime of each single component of the PANOPTESEC System.	Ensure that the system administrator can manage and optimize each component of the PANOPTESEC system easily and efficiently.	Modular architecture can sometimes be complicated to manage and optimize for system administrator. The PANOPTESEC system must be design to ease management and optimization.	2	1	1
CMP009	XML and JSON SHOULD be used as formats for data object exchanges.	Ensure that data objects exchanges are done using simple and standard formats.	Formats for data object exchange can be difficult to design and can be hard to debug. Using XML and JSON	2	2	1

			eases development.			

Table 11: Compatibility Non-Functional Requirements

8.3 Usability Requirements

Non-functional Usability Requirements are related to the *degree to which* the PANOPTESEC system *can be used by specified users to achieve specified goals with effectiveness, efficiency and satisfaction in a specified context of use* [2]. It encompasses appropriateness recognizability, learnability, operability, user error protection, user interface aesthetics and accessibility. Non-functional Usability Requirements unique id begins with USG.

id	Description	Goal	MainPurpose	Importance	Reachability	Version
USG001	The PANOPTESEC user interface and visualization system MUST exist in various versions, each version being suitable to the mission of each identified type of user.	Ensuring that each type of user will benefit from visualization and interfaces that are suited to their mission.	Not all users need the same kind of information and control on the system. The PANOPTESEC system MUST offer to each of the adequate visualizations, interfaces and interactions.	3	3	1

USG002	Usability of the PANOPTESEC system MUST be verified and improved through regular validation by end users.	Ensuring that the various users can efficiently use the system.	There is currently no magic recipe to design really efficient visualization, interfaces and interactions. Users' feedback must be used regularly to improve and evaluate PANOPTESEC prototypes.	3	3	1
USG003	The PANOPTESEC user interface and visualization component SHOULD be reactive to allow efficient user interactions.	Ensuring that users will not be frustrated by non-responsive interfaces.	Non-responsive interfaces have been showed to be one of the biggest causes of user frustration. The PANOPTESEC system must therefore be responsive enough so as to not cause frustration.	2	3	1

Table 12: Usability Non-Functional Requirements

8.4 Reliability Requirements

Non-functional Reliability Requirements are related to the degree to which the PANOPTESEC system performs specified functions under specified conditions for a specified period of time [2]. It encompasses maturity, availability, fault tolerance and recoverability. Non-functional Reliability Requirements unique id begins with RLB.

id	Description	Goal	MainPurpose	Importance	Reachability	Version
RLB001	Unit test cases MUST be created for each PANOPTESEC component.	Ensure respect of specifications and non-regression.	Having unit test case will ensure that developers respect specifications and that no regression happens when	3	2	1

			code is updated.			
RLB002	Unit test cases MUST be updated during the PANOPTESEC project according to results from experimentation.	Ensure that the tests are up to date with new specifications/features.	Having an up-to-date set of unit test cases allows verifying that software was correctly fixed if necessary and those new features have been correctly implemented.	3	2	1
RLB003	Updated unit test cases MUST be performed before any integration to ensure non-regression.	Ensure that no regression is introduced at a new integration.	Given the size of the project, it is fundamental that each piece of software is check against regression before any integration.	3	2	1
RLB004	The PANOPTESEC architecture SHOULD be designed to tolerate faults in any of its components.	Ensure that a crashing component will not cause a crash of the full PANOPTESEC system.	As problems may happen in any piece of software, it is important that these problems stay as local as possible and that a crash of a given component does not lead to a crash of the full system.	2	3	1

RLB005	In operational contexts, redundancy SHOULD be provided for databases in the PANOPTESEC system.	Ensure that the collected data will not be lost in case of a problem on the hardware/system hosting the database.	As hardware/system problems can happen, it is important in operational context to enforce redundancy of the database so as to ensure that the database remains available even if one of the machines that host the database endures and hardware/system failure.	2	1	1
RLB006	In operational contexts, databases in the PANOPTESEC system MUST be regularly backed-up.	Ensure that the database can be restored in case of problem.	Self-explanatory.	3	1	1
RLB007	The PANOPTESEC system MUST not impact the operational environment (i.e., the monitored or protected systems) when experiencing a failure.	Ensure that the PANOPTESEC will not be a source of vulnerability for the monitored system.	Self-explanatory.	3	1	1

RLB008	Recovery time of any PANOPTESEC component SHOULD be in the order of minutes.	Ensure that the failure of a component will not cause this component to be unavailable for more than a few minutes.	A component of the PANOPTESEC system that stays unavailable for too long could prevent the whole PANOPTESEC system from performing its intended tasks. It should be possible to restart components rapidly to avoid too long service interruption.	2	1	1
RLB009	Data Collection and Response Mitigation Actions of the PANOPTESEC system on the monitored system MUST not trigger events that would be detected as malicious activity (e.g., causing an Intrusion Detection System to raise an alert).	Ensure that the PANOPTESEC system will not cause alerts to be raised, which could even lead to an infinite loop of reaction/detection.	Self-explanatory.	3	3	1
RLB010	To avoid PANOPTESEC processing issues (e.g., race conditions or processing locks), the proactive and reactive response chains SHOULD use the same data	Ensure that the data used by the PANOPTESEC system for computation are consistent.	Using different version of the knowledge the PANOPTESEC system has of the monitored system could lead to inconsistencies, processing locks and race condition. To avoid this, the whole instance	2	3	1

	representing the state of the Monitored System(s) as an input during the whole instance of a given computation.		of a given computation must be performed on the same snapshot.			
RLB011	Each instance of a computation in the proactive and reactive response chains MUST be performed on the most recently completed data collection and correlations results from the data collection and correlation components representing the most up to date state of the monitored system(s). For example, the most recently computed values for the Network Inventory, Vulnerability Inventory, Reachability Matrix and Low Level Correlation.	Ensure that the results of the computations in the PANOPTESEC system are performed on the freshest data available.	Performing computations on old data could lead, for instance, to inconsistent response proposal. Computation on the freshest available data reduces this risk.	3	3	1

RLB012	Control loops that may result from interaction between components of the PANOPTESEC System MUST be identified.	Ensuring that the control loops inside the PANOPTESEC system are identified.	Control loops can cause numerous undesirable behaviors such as system instability. It is therefore necessary to identify them.	3	3	1
RLB013	Control loops that may result from interaction between components of the PANOPTESEC System and the monitored system(s) MUST be identified.	Ensuring that the control loops between components of the PANOPTESEC system and the monitored system are identified.	Control loops can cause numerous undesirable behaviors. It is therefore necessary to identify them.	3	3	1
RLB014	For all control loops identified for the PANOPTESEC System, including those between the PANOPTESEC System and the monitored system(s), their consequences MUST be evaluated.	Ensuring that the risks associated to the control loops that exist in the PANOPTESEC system are controlled.	Because control loops cannot always be avoided, it is important to analyze their potential consequences so as to mitigate undesirable behavior	3	3	1

Table 13: Reliability Non-Functional Requirement

8.5 Security Requirements

Non-functional Security Requirements are related to *the degree to which* the PANOPTESEC system *protects information and data so that persons or other products or systems have the degree of data access appropriate to their types and levels of authorization* [2]. It encompasses confidentiality, integrity, non-repudiation, accountability and authenticity. Non-functional Security Requirements unique id begins with SEC.

id	Description	Goal	MainPurpose	Importance	Reachability	Version
SEC001	The correlation results from the PANOPTESEC system SHOULD be stored in encrypted form.	Ensure that the confidentiality of correlation results of the PANOPTESEC system is ensured.	Correlation results of the PANOPTESEC system would be very valuable information for an attacker. Encrypting them makes it more difficult for an attacker to access them.	2	1	1
SEC002	Devices that implement the PANOPTESEC system components SHOULD limit services exposure.	Ensure the PANOPTESEC system components limit their service exposure to the strict minimum.	Limiting service exposure reduces the attach surface. It makes it more difficult for an attacker to compromise the PANOPTESEC system components.	2	1	1
SEC003	Communications between the PANOPTESEC System components SHOULD be authenticated.	Ensure that an attacker cannot modify data exchanged by the PANOPTESEC system components.	Tampering with communications between the PANOPTESEC system components would allow an attacker to go undetected or to cause inadequate responses. Therefore, their authenticity must be enforced.	2	2	1

SEC004	Communications between the PANOPTESEC system components SHOULD be encrypted.	Ensure that the confidentiality of communications between the PANOPTESEC system components is ensured.	Communications between the components of the PANOPTESEC system would be very valuable information for an attacker. Encrypting them makes it more difficult for an attacker to access them.	2	2	1
SEC005	User access to the PANOPTESEC system SHOULD require authentication based on individual user identification and password.	Ensure that the access by users to the PANOPTESEC system is controlled.	Access to the PANOPTESEC system by an attacker would for instance allow him or her to gain precious information on the monitored system, to tamper with it. Access to the PANOPTESEC system must therefore be controlled.	2	2	1
SEC006	The design and implementation of the PANOPTESEC system SHOULD support a future Common Criteria evaluation at the level of Evaluation Assurance Level 2 (EAL2).	Ensure that the PANOPTESEC project can lead to a product.	Common Criteria evaluation is required for systems to be used in some context. Design and implementation of the PANOPTESEC system must not prevent a future Common Criteria evaluation at the level of Evaluation Assurance Level 2 (EAL2).	2	2	1

Table 14: Security Non-Functional Requirements

8.6 Maintainability Requirements

Non-functional Maintainability Requirements are related to the degree of effectiveness and efficiency with which the PANOPTESEC system can be modified by the intended maintainers [2]. It encompasses modularity, reusability, analyzability, modifiability and testability. Non-functional Maintainability Requirements unique id begins with MNT.

id	Description	Goal	MainPurpose	Importance	Reachability	Version
MNT001	The PANOPTESEC System MUST be modular and decomposed in different components in order to improve maintainability.	Ensure that the PANOPTESEC system can be easily maintained even when its various components evolve and new features are implemented.	Maintaining a project comprising multiple technologies provided by multiple partners can be difficult. A modular architecture helps maintainability.	3	2	1
MNT002	The PANOPTESEC data model SHOULD be designed to support integration with new data sources in the monitored system(s)	Ensure that new data sources having different formats can be added to the PANOPTESEC system.	While a set of data sources have already been identified for the PANOPTESEC system, new types of data sources will certainly appear as they provide valuable information. It SHOULD be possible to support integration of new data sources in the PANOPTESEC project.	2	2	1

MNT003	The PANOPTESEC System SHOULD provide a unique configuration environment to ease the maintenance of the deployed components.	Ensure that the PANOPTESEC system can be easily deployed, managed and configured by system administrators.	Systems that are too complex to deploy, manage and configure are rarely adopted. The PANOPTESEC system SHOULD be easy to deploy, manage and configure.	2	2	1
MNT004	The PANOPTESEC System SHOULD be comprised of a fully integrated system of functions from detection to automated response recommendation and actuation.	Ensure that the integration of the PANOPTESEC systems components provide all the required functionalities.	Self-explanatory.	2	2	1

Table 15: Maintainability Non-Functional Requirements

8.7 Portability Requirements

Non-functional Portability Requirements are related to degree of effectiveness and efficiency with which the PANOPTESEC system can be transferred from one hardware, software or other operational or usage environment to another [2]. It encompasses adaptability, installability and replaceability. Non-functional Portability Requirements unique id begins with PRT.

id	Description	Goal	MainPurpose	Importance	Reachability	Version
PRT001	PANOPTESEC Components SHOULD be developed in a language that is portable between most current operating systems (e.g., JAVA).	Ensure that the PANOPTESEC system can be easily ported to the most current operating systems.	OS independence eases adoption of a technology. For the PANOPTESEC system to be widely adopted, it SHOULD be developed in a language that can run on the various most current operating systems.	2	2	1
PRT002	JAVA compliant interfaces MUST be provided by PANOPTESEC Components not written in JAVA.	Ensure that PANOPTESEC components can interact with and be controlled through JAVA applications.	While some components may need to be written in specifically suited languages, a common language is required for integration is to be used. JAVA being well known for being portable, JAVA compliant interfaces MUST be provided by PANOPTESEC Components not written in JAVA.	3	2	1
PRT003	PANOPTESEC Components SHOULD NOT require Operating System specific libraries.	Ensure that the PANOPTESEC system can be easily ported to the most current operating systems.	Requiring libraries that are specific to a given OS for a given component would bind this PANOPTESEC component to a specific OS. This should be avoided.	2	2	1

PRT004	PANOPTESEC Components design MUST follow a component-oriented model in order to enhance reuse and separation of concerns.	Ensure components separation of concerns and reusability.	Component-oriented architectures ease integration, separation and reusability. This is particularly desirable in medium-to-large software systems such as the PANOPTESEC system.	3	2	1
PRT005	PANOPTESEC Component designs MUST offer a clear and stable set of interfaces for use by other internal or external components.	Ensure that a given component evolution will have a limited impact on the rest of the PANOPTESEC system.	While PANOPTESEC components will evolve all along the project, they MUST be easy to integrate. Therefore, their interfaces MUST stay stable even if the inner parts of components evolve a lot.	3	2	1
PRT006	It SHOULD be possible to host the various PANOPTESEC Components in virtual machines.	Ensure that the PANOPTESEC system can be deployed in IaaS architecture.	Being able to host the various components of the PANOPTESEC system in virtual machines eases deployment both in operational contexts and for demos.	2	2	1

Table 16: Portability Non-Functional Requirements

9 CONCLUSIONS

In this document, we presented the methodology followed to identify stakeholders as well as to elicit, analyze, model, track, ensure coverage, validate and manage functional and non-functional requirements in the PANOPTESEC project. We also presented the PANOPTESEC functional and non-functional requirements.

9.1 Significant results achieved

This document ensures that all members of the PANOPTESEC consortium share a common understanding of the objectives of the project. The PANOPTESEC functional and non-functional requirements will be the baseline for the PANOPTESEC consortium. It will be used to guide project decisions, decide priorities and assess its results.

9.2 Recommendations

Functional and non-functional requirements identified in this document are fundamental guidelines for the PANOPTESEC project. Importance 3 requirements should be adressed first, if possible in the first iterations of the project. At each iteration, the PANOPTESEC consortium must check the requirements that are satisfied. Requirements may be regularly updated and new requirements should be added according, to end users feedback.

9.3 Deliverable validation

The validation of the operational requirements has been carried out through a series of actions:

- The cyclic process of requirements collection permitted permanent review the PANOPTESEC consortium partners. Many interactions occurred with members of WP3, WP4, WP5 and WP6 to ensure common understanding. ACEA also verified that the functional requirements were complete.
- Feedback from the reviewers during the First Period Review, 11th December 2014 and also specified in a written report was taken into account.
- A quality assurance review process (both peer review quality assurance [18] and requirement review quality assurance [19]) has been carried out on version 1.8 of this document.
- The External Advisory Board provided feedback on version 1.8 of this document. Scenarios have been updated accordingly.

10 REFERENCES

[1] S. Bradner, *RFC 2119: Key words for use in RFCs to Indicate Requirement Levels*, March 1997.

[2] ISO. ISO/IEC 25010:2011 *Systems and software engineering -- Systems and software Quality Requirements and Evaluation (SQuaRE) -- System and software quality models*, 2011.
[3] ISO. ISO 9241-210:2010 *Human-centered design for interactive systems,* 2010.
[4] ISO. ISO/IEC 27001:2013 - *Information security management*, 2013.
[5] S. Blomkvist, *User-Centred Design and Agile Development of IT Systems*. Licentiate thesis, Department of Information Technology, Uppsala University, December 2006
[6] B.W. Boehm, *A spiral model of software development and enhancement*. Computer, Vol. 21, No. 5, pp. 61–72, 1988.
[7] A. Dix, *Human-computer interaction*. Prentice hall, 2004.
[8] Daniel Galin, *Software Quality Assurance: From Theory to Implementation*, Pearson Addison-Wesley, 2003.
[9] The PANOPTESEC Consortium, *PANOPTESEC D2.1.1. – Deficiencies Evaluation v1.0*, April 2014.
[10] The PANOPTESEC Consortium, *PANOPTESEC D3.1.1 – System High Level Preliminary Design*, march 2015.
[11] Eclipse.org, *About Papyrus*, https://www.eclipse.org/papyrus/, last accessed on 15/03/2015.
[12] The PANOPTESEC Consortium, Configuration Management Plan.
[13] The PANOPETSEC Consortium, Grant Agreement for Collaborative Project, Annex 1 – Description of Work.
[14] European Commission, ICT – Information and Communication Technologies, Work Program 2013.
[15] ENISA, ENISA Threat Landscape, *Responding to the Evolving Threat Environment*, 2012.
[16] The PANOPTESEC Consortium, *Scenario Template*, available on the PANOPTESEC SVN.
[17] The PANOPTESEC Consortium, *PANOPTESEC Project Handbook*, available on the PANOPTESEC SVN.
[18] The PANOPTESEC Consortium, *PANOPTESEC Peer Review Quality Assurance checklist*, available on the PANOPTESEC SVN.
[19] The PANOPTESEC Consortium, *PANOPTESEC Requirement Review Quality Assurance checklist*, available on the PANOPTESEC SVN.

ANNEX A: USER SCENARIO 1, ATTACKS TO COMMAND AND CONTROL NETWORKS AND SYSTEMS OF A CRITICAL INFRASTRUCTURE

Scenario ID:	UserScenario01		
Scenario name:	Attacks to Command and Control networks and systems of a Critical Infrastructure		
Created by:	ACEA, RHEA	**Last updated by:**	RHEA
Date created:	16/02/2015	**Date last updated:**	11/03/2015

Objective:	The demonstration objective is to show the typical criticalities caused by the unavailability, unserviceability or subversion of the networks and systems comprising a Command and Control center caused by cyber attacks targeting known vulnerabilities. Cyber security operations personnel are equipped: 1. In a proactive way to monitor, analyze, plan and execute mitigation actions in response to known vulnerabilities to reduce the attack surface and protect mission critical services; and 2. In a reactive way to monitor, analyze, plan and execute mitigation actions in response to identified cyber incidents to limit the impact of cyber incidents on mission critical services.
Proactive or Reactive?	Both
Supported business function:	Operative management, maintenance and development of the Critical Infrastructure (e.g. electricity / water distribution management)
Description:	Command and Control (C&C) centers and dedicated networks are used to manage SCADA devices and networks that are operating all Critical Infrastructures (e.g. electricity / water distribution systems) This macro-scenario evaluates the ongoing cyber security status of the C&C center of a Critical Infrastructure having some hostile

	or detrimental cyber events applied to its communication network and eventually systems and services operating critical C&C functions (i.e. network based attacks, whether internal or external, leading to compromise of communications or services supporting Critical Infrastructure management). If the C&C center is unable to properly manage the SCADA network it is responsible for, the Critical Infrastructure will continue to operate using previously programmed rules or scripted conditional actions stored inside the SCADA servers locally present in some sub-sites. This situation is normal due to possible connection problems and outages always present in large and geographically dispersed SCADA installations. However, the range of acceptability for this condition varies depending on the real world situation, both in term of timing, number, criticality of unreachable nodes and/or missing pieces of SCADA information. Without any means for the C&C center to act on these unreachable nodes, or check their status, the operators will call for repairs while relying on the built-in resilience of the SCADA system itself. Possibly, operator personnel could receive notifications of service failures from field-based personnel, police or customers (e.g. phone calls, emails, support requests). In the worst case, should the C&C center lose the capability to manage the SCADA network and devices due to cyber attackers taking control of SCADA servers/devices, the attackers could cause critical damage to the infrastructure devices and cause catastrophic disruption of services delivery. If too many critical nodes of the SCADA network are out of control (e.g. in this macro-scenario this is due to an attack recognized by the PANOPTESEC system), it is possible that default rules and scripted conditional actions inside the SCADA servers and devices that drive PLCs could fail unpredictably when handling complex situations: these conditions are out of the scope of this macro-scenario. This macro-scenario encompasses continuous security monitoring capabilities operating in both a proactive and reactive model. Proactive security monitoring is intended to improve the security posture of the environment through prioritized response to known vulnerabilities. Reactive security monitoring is intended to respond to cyber attacks that may hinder or prevent the ability to control and remotely manage the Critical Infrastructure.

Business impact:	Complete or partial loss of control of the Critical Infrastructure due to the disruption of its Command and Control network capabilities; Potential for direct, indirect or collateral damage to the Critical Infrastructure itself. Loss of awareness of the ongoing status of the Critical Infrastructure (e.g. network parameters and measurements, power grid balancing status, water distribution measurements) Loss of capability to support maintenance operations (e.g. programmed changes or timed power grid rebalancing) Loss of capability to control or guarantee the core business services (e.g. electricity/water distribution)
Stakeholder actors (including user roles):	The following represent the general groups of stakeholders involved in the use of the security monitoring and response functions: **Business Stakeholders/Owners:** Executive level functions interested in understanding the security status of the business (mission) processes. **Operational Stakeholders:** Collectively, personnel responsible for the ongoing service and operational delivery of business (mission) processes (e.g., SCADA operators, network operators, security operators). The following represent the specific **user roles** involved in the use of the PANOPTESEC system: **PANOPTESEC Security Operator:** Primary users of the PANOPTESEC system. Operators have both proactive and reactive responsibilities. Proactive functions include reviewing vulnerabilities within the monitored system, reviewing potential mission impact, review and selection of mitigation actions and their execution. Reactive functions include reviewing indications of suspected cyber attacks, reviewing potential mission impacts, review and selection of mitigation actions and approval of execution;

	Network Operator: In some instances, the approved mitigation actions executed by PANOPTESEC will require intervention on the part of Network Operator staff to implement the chosen mitigation action (e.g., implementation of patches or making changes to system configuration); **SCADA Operator:** Users involved in management of the SCADA devices and environment; **ICT Operator:** Users involved in management of the ICT devices and environment; **PANOPTESEC System Manager:** Involved in setup and configuration of the data sensors interface with the PANOPTESEC system as well as any pre-configuration or configuration changes needed by the PANOPTESEC system (e.g., input the list of pre-approved mitigation actions); **Business Owner:** Executive level function interested in understanding the security status of the business (mission) processes; **Monitored System**: Includes SCADA systems (e.g., database and/or SCADA servers, Front End Gateways, etc.) and ICT systems (e.g., Network devices, database servers, Domain Name Servers, computers used to access the infrastructure to perform operational roles, etc.); **Cyber sensors:** Sources of cyber relevant data within the Monitored System used by PANOPTESEC for security analysis and mitigation action planning and execution.
Threat agent actors:	**Corporations:** in a competitive business environment adversaries may use cyber tools to acquire new market shares from others (may use Cyber spies, Cybercriminals or bribe employees) **Cyber Vandal:** derives thrills from intrusion or destruction of cyber property, without agenda (e.g. web site defacers) **Cyber warrior:** attacker with high skills and significant resources, may be able to cause major disruption on local/regional/national scale **Cyber spy:** spy that acts individually or in small groups, may be hired from competitors or other parties, possessing high cyber skills and access to significant resources. **Cybercriminal:** may act individually or on behalf of others (e.g. mobsters and organized crime, business competitors) and uses

	his medium/high level cyber skills to attack / destroy cyber assets, abuse or steal resources. He acts only for profit. **Cyberterrorist:** a terrorist who relies on the use of cyber methods to support a specific socio-political agenda, may be alone or organized in small groups, acts on order or on opportunity targets (e.g. Al Qaeda, ISIS) **Employee:** current or former employee/operator of the system **Hacktivist:** highly motivated activist with cyber skills, may eventually act in an organized crew or party, depending on role and personal capabilities (e.g. Anonymous) **Mobster:** manager of organized crime organization with significant resources **Nation-state:** a sovereign territory with significant resources to cause harm (may support Cyberterrorists or use Cyber warriors or even Cybercriminals)
Assumptions:	Access to public or private WAN networks that the user agency is actually using, (e.g. network connections from RTU substations in the field to the SCADA Servers in the C&C site)
Preconditions:	C&C center is operative; threat agents have access to the external and/or internal networks and systems. PANOPTESEC system is operative and acquires information concerning the Monitored Systems. Supporting data is provided by non-monitored system references (e.g. public vulnerability databases).
Normal flow of events:	**SCADA Operations:** The SCADA Operators perform regular operations to manage the Critical Infrastructure using the C&C system that connects to the SCADA devices in the field. All the automated safeguards and balancing actions are working normally and are available. Overall, the systems are operating normally (or self-balancing correctly); if minor problems are present they are normal technical issues. **Security (PANOPTESEC) Operations (MAPE cycle): [Monitor]** PANOPTESEC Security Operators review the security status of the Monitored System (SCADA and ICT environment). **[Analyze]** Security status indicators may note the presence of one or more system vulnerabilities due to known software security flaws as posted by openly available vulnerability advisory services. Attack paths from hypothetical attack sources (both internal and external) to known mission critical systems are analyzed and the

	impact on critical business functions (e.g., energy distribution) is assessed resulting in a quantified risk assessment. **[Plan]** Prioritized mitigation actions are presented to the PANOPTESEC Security Operators. Mitigation actions may consist of one or more discrete actions that collectively improve the security status of the Monitored System (e.g., patch deployment or other system reconfiguration). **[Execute]** Mitigation actions are selected and executed by the PANOPTESEC Security Operators resulting in automated deployment of mitigation actions where possible (e.g., firewall reconfigurations) or otherwise issuing instructions to Network and ICT Operators for follow-up deployment of mitigations (e.g., patch deployment). PANOPTESEC Security Operators also provide periodic status reports to Business Owners concerning the security status of their business (mission) operations. **Network and ICT Operations:** Network and ICT Operators receive notifications of mitigation actions from the PANOPTESEC Security Operators and take appropriate steps to implement the requested security mitigation actions. **Business owners:** Business Owners receive periodic status reports concerning the security status of their business (mission) operations and provide oversight to SCADA and ICT system operations.
Compromise:	One or more threat agents exploit one or more vulnerabilities or use legitimate access rights to penetrate into, or to or otherwise attack one or more assets used for C&C of the Critical Infrastructure, examples are: • *Compromise a gateway of SCADA commands flow* • *Compromise a server of SCADA commands* • *Compromise data flow to gain arbitrary view/control* • *Compromise an unspecific host in C&C network as botnet Zombie host* *Due to these actions, the C&C systems are either:* *1. Unable to reach / send SCADA commands to a large number of RTUs/PLCs and thus cannot perform regular operations to manage the targeted Critical Infrastructure devices; or*

	2. Controlled by the cyber threat agents allowing them to execute arbitrary functions The PANOPTESEC system detects impaired conditions of the monitored systems.
Frequency of occurrence:	Low, but at the moment it is not possible to associate past historical failures to specific cyber attacks
Likelihood (probability) of success:	High (at least in the user agency due to the actual C&C network structure and topology)
Loss expectancy:	More than tens of thousands of Euros per minute (may depend on the number and type of devices whose operations are hindered by hostile actions)
Consequences:	Legal exposure, economic loss, reputation loss, regulation compliance loss, potentially massive social impact.
Compromised flow of events:	One or more threat agents target the C&C center of the Critical Infrastructure using one or more attack vectors / types (e.g. sending exploits to servers and communication devices, using DoS to silence the servers, use buffer overflows to subvert server services exposed, etc.). One or more attacks complete successfully and the attacker gains and/or escalates privileges, compromises other assets or blocks the communications between the C&C center and the Critical Infrastructure. After a successful compromise, the C&C center is not able to manage a significant part of the SCADA devices of the Critical Infrastructure. In the worst case, a significant part of the SCADA devices of the Critical Infrastructure are not under (exclusive) control of the C&C center; they act differently compared to the original programming and pre-sets; some compromised SCADA servers may be used to execute arbitrary functions and commands on the SCADA devices in the field. **Security (PANOPTESEC) Operations (MAPE cycle): [Monitor]** PANOPTESEC Security operators review alerts presented in the form of security status of the Monitored System (SCADA and ICT environment). **[Analyze]** Security status indicators note the presence of one or more cyber incidents aligned with previously identified attack paths from hypothetical attack sources (both internal and external) to known mission critical systems.

	Potential impact on critical business functions (e.g., energy distribution) is assessed resulting in a quantified risk assessment. **[Plan]** Prioritized reactive mitigation actions are presented to the PANOPTESEC Security Operator. Reactive mitigation actions may consist of one or more discrete actions (e.g., exploited ports and protocols are blocked, exploited services are disabled). **[Execute]** Reactive mitigation actions are selected and executed by the PANOPTESEC Security Operators resulting in automated deployment where possible (e.g., firewall reconfigurations) or otherwise issuing instructions to Network and ICT Operators for follow-up deployment of mitigation actions (e.g., system reconfigurations outside PANOPTESEC Security Operator control). PANOPTESEC Security Operators also provide periodic status reports to Business Owners concerning the security status of their business (mission) operations. **Network and ICT Operations:** Network and ICT Operators receive notifications of mitigation actions from the PANOPTESEC Security Operators and take appropriate steps to implement the requested reactive mitigation actions. **Business Owners:** Business Owners receive periodic status reports concerning the security status of their business (mission) operations and provide oversight to SCADA and ICT system operations.
Impact of compromise	Possible legal and financial impacts arise as consequences of the loss of control of the Critical Infrastructure, mostly due to the loss of regulation compliance. Corporation may be fined. In the worst case, there is potential social impact: minor/major blackouts and clean water shortages. They may require a long time to be assessed and resolved as may be necessary to physically reach, reset/reprogram the RTUs/PLCs.
Detection indicators:	C&C center loses established network connections or can't accept/establish new connections to RTUs of the Critical Infrastructure. Security alerts are logged by security software/devices (e.g., firewall logs, intrusion detection system alerts, etc.) and PANOPTESEC system correlates them to on-going attacks
Analysis indicators:	Possible attack paths should support PANOPTESEC Security Operators to understand if the actual situation is similar to an

	attack to the C&C network of the Critical Infrastructure.
Valid mitigation options:	Notification and visibility of possible ongoing attacks are the top priority, but mitigation options could actually be available or not depending on the target(s). Depending the situation, valid mitigation actions may include, among others: • Patch deployment, system update; • Port and protocol reconfigurations; • Routing reconfigurations; • Services shut down.
Invalid mitigation options:	Any major blocking action on the network is normally unwanted but it may actually depend on the asset(s)/node(s) being attacked and from the overall situation. In proactive operational case (i.e., response to identified vulnerabilities), no actions that would disrupt the SCADA system operation would be tolerated, unless it can be timed to coincide with regular system maintenance cycles. In reactive operational case (i.e., response to identified cyber attacks), actions that may temporarily disrupt the SCADA system operation may be tolerated if these can be managed in a controlled manner.
Mitigation flow of events:	Mitigation actions are selected and executed by the PANOPTESEC Security Operator resulting in automated deployment of mitigation actions where possible (e.g., firewall reconfigurations) or otherwise issuing instructions to Network and ICT Operators for follow-up deployment of mitigations (e.g., system reconfigurations outside PANOPTESEC Security Operator control). PANOPTESEC Security Operators also provide periodic status reports to Business Owners concerning the security status of their business (mission) operations. **Network and ICT Operations**: Network and ICT Operators receive notifications of mitigation actions from the PANOPTESEC Security Operators and take appropriate steps to implement the requested security mitigation actions.
Post conditions:	After the application of the mitigation actions, the SCADA Operators regain control: all the previously affected systems are restored to proper operation and continue to maintain traces and audit logs.

Includes:	This macro-scenario is not referencing directly other scenarios, but can be specialized/customized obtaining more specific sub-scenarios (e.g. depending on the threat agents, attacks, number of assets compromised, duration of the attack, etc.) so it can be referenced.
Priority (define?):	Importance of scenario is High and the risk may be acceptable or not depending on the role of the targeted nodes inside the C&C center network. It should be present in the final list of demonstration scenarios.
Special requirements:	None.
Simulation Requirements:	The Simulation Environment must be able to properly emulate the existing C&C network of the Critical Infrastructure and provide appropriate sensors to support data collection requirements of the PANOPTESEC system.
Notes and Issues:	None.

ANNEX B: USER SCENARIO 2, ATTACKS TO THE SCADA EQUIPMENT/DEVICES OF A CRITICAL INFRASTRUCTURE, PERFORMED THROUGH ITS SCADA COMMAND AND CONTROL NETWORK

Scenario ID:	UserScenario02		
Scenario name:	Attacks to the SCADA equipment/devices of a Critical Infrastructure, performed through its SCADA Command and Control network, that have a relevant social impact		
Created by:	ACEA, RHEA	**Last updated by:**	RHEA
Date created:	16/02/2015	**Date last updated:**	11/03/2015

Objective:	The demonstration objective is to show the typical criticalities caused by the unavailability, unserviceability or subversion of the networks and systems comprising a Command and Control center caused by cyber attacks targeting known vulnerabilities of the SCADA equipment/devices of a Critical Infrastructure, performed through its SCADA Command and Control network, that have a relevant social impact. Cyber security operations personnel are equipped: • In a proactive way to monitor, analyze, plan and execute mitigation actions in response to known vulnerabilities to reduce the attack surface and protect mission critical services; and • In a reactive way to monitor, analyze, plan and execute mitigation actions in response to identified cyber incidents to limit the impact of cyber incidents on mission critical services.
Proactive or Reactive?	Both
Supported business function:	Operative management, maintenance and development of the Critical Infrastructure (e.g. electricity / water distribution management)

Description:	Command and Control centers and dedicated networks are used to manage SCADA devices and networks that are operating all Critical Infrastructures (e.g. electricity / water distribution systems) This macro-scenario evaluates the ongoing status of a Critical Infrastructure having some hostile or detrimental events applied to its communication network (i.e. external network facing RTUs devices in the field, thus used to connect them to the Command and Control center) and on the SCADA servers/devices scattered in the field (not on the Command and Control center itself). This macro-scenario encompasses several possible actions that can hinder or prevent the operation of the targeted Critical Infrastructure and the relevant/applicable mitigation actions. This macro-scenario encompasses continuous security monitoring capabilities operating in both a proactive and reactive model. Proactive security monitoring is intended to improve the security posture of the environment through prioritized response to known vulnerabilities. Reactive security monitoring is intended to respond to cyber attacks that may hinder or prevent the ability to control and remotely manage the Critical Infrastructure.
Business impact:	Complete or partial loss of control of the Critical Infrastructure due to the disruption of its devices; Direct damage to the Critical Infrastructure devices occurs. Loss of awareness of the ongoing status of the Critical Infrastructure (e.g. network parameters and measurements, power grid balancing status, water distribution measurements) Loss of capability to support maintenance operations (e.g. programmed changes or timed grid rebalancing) Loss of capability to control or guarantee the core business services (e.g. electricity/water distribution) Massive blackouts or clean water shortages are possible.

Stakeholder actors (including user roles):	The following represent the general groups of stakeholders involved in the use of the security monitoring and response functions: **Business Stakeholders/Owners:** Executive level functions interested in understanding the security status of the business (mission) processes. **Operational Stakeholders:** Collectively, personnel responsible for the ongoing service and operational delivery of business (mission) processes (e.g., SCADA operators, network operators, security operators). The following represent the specific **user roles** involved in the use of the PANOPTESEC system: **PANOPTESEC Security Operator:** Primary users of the PANOPTESEC system. Operators have both proactive and reactive responsibilities. Proactive functions include reviewing vulnerabilities within the monitored system, reviewing potential mission impact, review and selection of mitigation actions and their execution. Reactive functions include reviewing indications of suspected cyber attacks, reviewing potential mission impacts, review and selection of mitigation actions and approval of execution; **Network Operator:** In some instances, the approved mitigation actions executed by PANOPTESEC will require intervention on the part of Network Operator staff to implement the chosen mitigation action (e.g., implementation of patches or making changes to system configuration); **SCADA Operator:** Users involved in management of the SCADA devices and environment; **ICT Operator:** Users involved in management of the ICT devices and environment; **PANOPTESEC System Manager:** Involved in setup and configuration of the data sensors interface with the PANOPTESEC system as well as any pre-configuration or configuration changes needed by the PANOPTESEC system (e.g., input the list of pre-approved mitigation actions); **Business Owner:** Executive level function interested in understanding the security status of the business (mission) processes; **Monitored System**: Includes SCADA systems (e.g., database and/or SCADA servers, Front End Gateways, etc.) and ICT

	systems (e.g., Network devices, database servers, Domain Name Servers, computers used to access the infrastructure to perform operational roles, etc.); **Cyber sensors:** Sources of cyber relevant data within the Monitored System used by PANOPTESEC for security analysis and mitigation action planning and execution.
Threat agent actors:	**Corporations:** in a competitive business environment adversaries may use cyber tools to acquire new market shares from others (may use Cyber spies, Cybercriminals or bribe employees) **Cyber Vandal:** derives thrills from intrusion or destruction of cyber property, without agenda (e.g. web site defacers) **Cyber warrior:** attacker with high skills and significant resources, may be able to cause major disruption on local/regional/national scale **Cyber spy:** spy that acts individually or in small groups, may be hired from competitors or other parties, possessing high cyber skills and access to significant resources. **Cybercriminal:** may act individually or on behalf of others (e.g. mobsters and organized crime, business competitors) and uses his medium/high level cyber skills to attack / destroy cyber assets, abuse or steal resources. He acts only for profit. **Cyberterrorist:** a terrorist who relies on the use of cyber methods to support a specific socio-political agenda, may be alone or organized in small groups, acts on order or on

	opportunity targets (e.g. Al Qaeda, ISIS) **Employee:** current or former employee/operator of the system **Hacktivist:** highly motivated activist with cyber skills, may eventually act in an organized crew or party, depending on role and personal capabilities (e.g. Anonymous) **Mobster:** manager of organized crime organization with significant resources **Nation-state:** a sovereign territory with significant resources to cause harm (may support Cyberterrorists or use Cyber warriors or even Cybercriminals)
Assumptions:	Access to public or private WAN networks that the user agency is actually using, (e.g. network connections from RTU substations in the field to the SCADA Servers in the C&C site)
Preconditions:	Command and Control system is operative, threat agents have access to the external networks (only outer attack surface) PANOPTESEC system is operative and acquires information concerning the Monitored Systems in the field. Supporting data is provided by non-monitored system references (e.g. public vulnerability databases).
Normal flow of events:	**SCADA Operations:** The SCADA Operators perform regular operations to manage the Critical Infrastructure using the C&C system that connects to the SCADA devices in the field. All the automated safeguards and balancing actions are working normally and are available. Overall, the systems are operating normally (or self-balancing correctly); if minor problems are present they are normal technical issues. **Security (PANOPTESEC) Operations (MAPE cycle): [Monitor]** PANOPTESEC Security Operators review the security status of the Monitored System (SCADA and ICT environment). **[Analyze]** Security status indicators may note the presence of one or more system vulnerabilities due to known software security flaws as posted by openly available vulnerability advisory services. Attack paths from hypothetical attack sources (both internal and external) to known mission critical systems are analyzed and the impact on critical business functions (e.g., energy distribution) is assessed resulting in a quantified risk assessment. **[Plan]** Prioritized mitigation actions are presented to the PANOPTESEC Security Operators. Mitigation actions may consist of one or more discrete actions that collectively improve the security status of the Monitored System (e.g., patch deployment or

	other system reconfiguration). **[Execute]** Mitigation actions are selected and executed by the PANOPTESEC Security Operators resulting in automated deployment of mitigation actions where possible (e.g., firewall reconfigurations) or otherwise issuing instructions to Network and ICT Operators for follow-up deployment of mitigations (e.g., patch deployment). PANOPTESEC Security Operators also provide periodic status reports to Business Owners concerning the security status of their business (mission) operations. **Network and ICT Operations:** Network and ICT Operators receive notifications of mitigation actions from the PANOPTESEC Security Operators and take appropriate steps to implement the requested security mitigation actions. **Business owners:** Business Owners receive periodic status reports concerning the security status of their business (mission) operations and provide oversight to SCADA and ICT system operations.
Compromise:	One or more threat agents exploit one or more vulnerabilities or use legitimate access rights to penetrate into assets of the Critical Infrastructure, examples are: • Compromise a gateway of SCADA Remote Unit in the field • Compromise SCADA Remote Unit to perform arbitrary command (not agree or showed from C&C system) • Compromise SCADA Remote Unit flow (or Gateways) to put a “men in the middle” host/gateway Due to these actions, an attacker could perform: • Command Action on critical infrastructure equipment with relative social impact • Send false data to the C&C system about real status of critical infrastructure equipment • Generate the “domino effect failure” (especially for electrical infrastructures) starting from one compromise Remote Unit The PANOPTESEC system detects impaired conditions of the monitored systems.
Frequency of	Low, but at the moment it is not possible to associate past

occurrence:	historical failures to specific cyber attacks
Likelihood (probability) of success:	High (at least in the user agency due to the actual C&C network structure and topology)
Loss expectancy:	More than tens of thousands of Euros per minute (may depend on the number and type of devices whose operations are hindered by hostile actions)
Consequences:	Legal exposure, economic loss, reputation loss, regulation compliance loss, massive social impact.
Compromised flow of events:	One or more threat agents target the Critical Infrastructure equipment using one or more attack vectors / types (e.g. sending exploits to servers and communication devices, using DoS to silence the servers, use buffer overflows to subvert server services exposed, etc.). One or more attacks complete successfully and the attacker gains and/or escalates privileges, compromises other assets or blocks the communications between the C&C center and the Critical Infrastructure devices (RTUs/PLC). After a successful compromise, the C&C center could not able to manage a significant part of the SCADA devices of the Critical Infrastructure. In the worst case, the SCADA devices of the Critical Infrastructure are not under (exclusive) control of the C&C center; they act differently compared to the original programming and pre-sets; some compromised SCADA servers may be used to execute arbitrary functions and commands on the SCADA devices in the field. **Security (PANOPTESEC) Operations (MAPE cycle): [Monitor]** PANOPTESEC Security operators review alerts presented in the form of security status of the Monitored System (SCADA and ICT environment). **[Analyze]** Security status indicators note the presence of one or more cyber incidents aligned with previously identified attack paths from hypothetical attack sources (both internal and external) to known mission critical systems. Potential impact on critical business functions (e.g., energy distribution) is assessed resulting in a quantified risk assessment. **[Plan]** Prioritized reactive mitigation actions are presented to the PANOPTESEC Security Operator. Reactive mitigation actions may consist of one or more discrete actions (e.g., exploited ports and protocols are blocked, exploited services are disabled). **[Execute]** Reactive mitigation actions are selected and executed by the PANOPTESEC Security Operators

	resulting in automated deployment where possible (e.g., firewall reconfigurations) or otherwise issuing instructions to Network and ICT Operators for follow-up deployment of mitigation actions (e.g., system reconfigurations outside PANOPTESEC Security Operator control). PANOPTESEC Security Operators also provide periodic status reports to Business Owners concerning the security status of their business (mission) operations. **Network and ICT Operations:** Network and ICT Operators receive notifications of mitigation actions from the PANOPTESEC Security Operators and take appropriate steps to implement the requested reactive mitigation actions. **Business Owners:** Business Owners receive periodic status reports concerning the security status of their business (mission) operations and provide oversight to SCADA and ICT system operations.
Impact of compromise	Possible legal and financial impacts arise as consequences of the loss of control of the Critical Infrastructure, mostly due to the loss of regulation compliance. Corporation may be fined. In the worst case, there is social impact: minor/major blackouts and clean water shortages. They may require a long time to be assessed and resolved as may be necessary to physically reach, reset/reprogram the RTUs/PLCs. Local/regional/national shutdown of power systems if the local/regional/national balancing system goes down as a consequence (domino effect). Huge legal and financial impacts arise as consequences: corporation will be fined or even excluded from actual/future tenders for these services and/or bankrupt.
Detection indicators:	C&C center loses established network connections or can't accept/establish new connections to RTUs of the Critical Infrastructure. Security alerts are logged by security software/devices (e.g., firewall logs, intrusion detection system alerts, etc.) and PANOPTESEC system correlates them to on-going attacks
Analysis indicators:	Possible attack paths should support PANOPTESEC Security Operators to understand if the actual situation is similar to an attack to the Critical Infrastructure device.
Valid mitigation	Notification and visibility of possible ongoing attacks are the top

options:	priority, but mitigation options could actually be available or not depending on the target(s). Depending the situation, valid mitigation actions may include, among others: • Patch deployment, system update; • Port and protocol reconfigurations; • Routing reconfigurations and/or ACL enabling • Force RTU device in the field to use a different type of connection
Invalid mitigation options:	Blocking ALL SCADA commands, including legitimate ones or isolate RTU from network node vector attack path if possible.
Mitigation flow of events:	Mitigation actions are selected and executed by the PANOPTESEC Security Operator resulting in automated deployment of mitigation actions where possible (e.g., firewall reconfigurations) or otherwise issuing instructions to Network and ICT Operators for follow-up deployment of mitigations (e.g., system reconfigurations outside PANOPTESEC Security Operator control). PANOPTESEC Security Operators also provide periodic status reports to Business Owners concerning the security status of their business (mission) operations. **Network and ICT Operations**: Network and ICT Operators receive notifications of mitigation actions from the PANOPTESEC Security Operators and take appropriate steps to implement the requested security mitigation actions.
Post conditions:	After the application of the mitigation actions, the SCADA Operators regain control: all the previously affected systems are restored to proper operation and continue to maintain traces and audit logs.
Includes:	This macro-scenario is not referencing directly other scenarios, but can be specialized/customized obtaining more specific sub-scenarios (e.g. depending on the threat agents, attacks, number of assets compromised, duration of the attack, etc.) so it can be referenced.
Priority (define?):	Importance of scenario is High and the risk may be acceptable or not depending on the role of the targeted nodes inside the C&C center network. It should be present in the final list of demonstration scenarios.
Special	None.

requirements:	
Simulation Requirements:	The Simulation Environment must be able to properly emulate the existing C&C network of the Critical Infrastructure and provide appropriate sensors to support data collection requirements of the PANOPTESEC system.
Notes and Issues:	None.

ANNEX C: USER SCENARIO 3, ATTACK TO ONE OR MORE NODES THAT OPERATES SOME IT SERVICES UNDERLYING A NON-CORE BUSINESS PROCESS.

Scenario ID:	UserScenario03		
Scenario name:	Attack to one or more nodes that operate some ICT services underlying a business process.		
Created by:	ACEA, RHEA	**Last updated by:**	RHEA
Date created:	16/02/2015	**Date last updated:**	11/03/2015

Objective:	The demonstration objective is to show the typical criticalities caused by the disruption of a business process due to unavailability, unserviceability or subversion of the ICT services and devices, eventually applying proactive or reactive mitigation actions until the underlying ICT services and the business process are fully restored. Cyber security operations personnel are equipped: • In a proactive way to monitor, analyze, plan and execute mitigation actions in response to known vulnerabilities to reduce the attack surface and protect mission critical services; and • In a reactive way to monitor, analyze, plan and execute mitigation actions in response to identified cyber incidents to limit the impact of cyber incidents on mission critical services.
Proactive or	Both

Reactive?	
Supported business function:	Operative management, maintenance and development of this business function, supported by any business process and IT infrastructure.
Description:	This macro-scenario encompasses actions aiming to hack into an ICT infrastructure made, for example, of files servers associated to the operational task or dedicated web servers. This macro-scenario encompasses continuous security monitoring capabilities operating in both a proactive and reactive model. Proactive security monitoring is intended to improve the security posture of the environment through prioritized response to known vulnerabilities. Reactive security monitoring is intended to respond to cyber attacks that may hinder or prevent the ability to control and remotely manage the Critical Infrastructure.
Business impact:	Complete or partial loss of delivery of the attacked business function due to malfunction of some business processes and/or underlying sub-processes or devices (i.e. web server of file servers).
Stakeholder actors (including user roles):	The following represent the general groups of stakeholders involved in the use of the security monitoring and response functions: **Business Stakeholders/Owners:** Executive level functions interested in understanding the security status of the business (mission) processes. **Operational Stakeholders:** Collectively, personnel responsible for the ongoing service and operational delivery of business (mission) processes (e.g., SCADA operators, network operators, security operators). The following represent the specific **user roles** involved in the use of the PANOPTESEC system: **PANOPTESEC Security Operator:** Primary users of the PANOPTESEC system. Operators have both proactive and reactive responsibilities. Proactive functions include reviewing vulnerabilities within the monitored system, reviewing potential mission impact, review and selection of mitigation actions and

	their execution. Reactive functions include reviewing indications of suspected cyber attacks, reviewing potential mission impacts, review and selection of mitigation actions and approval of execution; **Network Operator:** In some instances, the approved mitigation actions executed by PANOPTESEC will require intervention on the part of Network Operator staff to implement the chosen mitigation action (e.g., implementation of patches or making changes to system configuration); **ICT Operator:** Users involved in management of the ICT devices and environment; **PANOPTESEC System Manager:** Involved in setup and configuration of the data sensors interface with the PANOPTESEC system as well as any pre-configuration or configuration changes needed by the PANOPTESEC system (e.g., input the list of pre-approved mitigation actions); **Business Owner:** Executive level function interested in understanding the security status of the business (mission) processes; **Monitored System**: Includes ICT systems (e.g., Network devices, database servers, Domain Name Servers, computers used to access the infrastructure to perform operational roles, etc.); **Cyber sensors:** Sources of cyber relevant data within the Monitored System used by PANOPTESEC for security analysis and mitigation action planning and execution.
Threat agent actors:	**Corporations:** in a competitive business environment adversaries may use cyber tools to acquire new market shares from others (may use Cyber spies, Cybercriminals or bribe employees) **Cyber Vandal:** derives thrills from intrusion or destruction of cyber property, without agenda (e.g. web site defacers) **Cyber warrior:** attacker with high skills and significant resources, may be able to cause major disruption on local/regional/national scale **Cyber spy:** spy that acts individually or in small groups, may be hired from competitors or other parties, possessing high cyber skills and access to significant resources. **Cybercriminal:** may act individually or on behalf of others (e.g. mobsters and organized crime, business competitors) and uses

	his medium/high level cyber skills to attack / destroy cyber assets, abuse or steal resources. He acts only for profit. **Cyberterrorist:** a terrorist who relies on the use of cyber methods to support a specific socio-political agenda, may be alone or organized in small groups, acts on order or on opportunity targets (e.g. Al Qaeda, ISIS) **Employee:** current or former employee/operator of the system **Hacktivist:** highly motivated activist with cyber skills, may eventually act in an organized crew or party, depending on role and personal capabilities (e.g. Anonymous) **Mobster:** manager of organized crime organization with significant resources **Nation-state:** a sovereign territory with significant resources to cause harm (may support Cyberterrorists or use Cyber warriors or even Cybercriminals)
Assumptions:	Access to public or private WAN networks that the user agency is actually using. Access to the internal and/or external Acea networks (e.g. Acea ICT network, DMZ network) servicing the business process
Preconditions:	Business process is operating normally. Threat agents have access to the network used from the IT service PANOPTESEC system is operative and acquires information concerning the Monitored Systems. Supporting data is provided by non-monitored system references (e.g. public vulnerability databases).
Normal flow of events:	**ICT Operations:** The ICT systems are operating normally. If minor problems are present they are normal technical issues. **Security (PANOPTESEC) Operations (MAPE cycle): [Monitor]** PANOPTESEC Security Operators review the security status of the Monitored System (ICT environment). **[Analyze]** Security status indicators may note the presence of one or more system vulnerabilities due to known software security flaws as posted by openly available vulnerability advisory services. Attack paths from hypothetical attack sources (both internal and external) to known mission critical systems are analyzed and the impact on critical business functions is assessed resulting in a quantified risk assessment. **[Plan]** Prioritized mitigation actions are presented to the PANOPTESEC Security Operators. Mitigation

	actions may consist of one or more discrete actions that collectively improve the security status of the Monitored System (e.g., patch deployment or other system reconfiguration). **[Execute]** Mitigation actions are selected and executed by the PANOPTESEC Security Operators resulting in automated deployment of mitigation actions where possible (e.g., firewall reconfigurations) or otherwise issuing instructions to Network and ICT Operators for follow-up deployment of mitigations (e.g., patch deployment). PANOPTESEC Security Operators also provide periodic status reports to Business Owners concerning the security status of their business (mission) operations. **Network and ICT Operations:** Network and ICT Operators receive notifications of mitigation actions from the PANOPTESEC Security Operators and take appropriate steps to implement the requested security mitigation actions. **Business owners:** Business Owners receive periodic status reports concerning the security status of their business (mission) operations and provide oversight to ICT system operations.
Compromise:	One or more threat agents exploit one or more vulnerabilities or use legitimate access rights to penetrate into, or to otherwise attack one or more ICT assets used in support of business functions. Due to these actions, the ICT Services are either: 1. Unable to reach / send / perform regular operation from IT services by related operator; or 2. Controlled by the cyber threat agents allowing them to execute arbitrary functions. The PANOPTESEC system detects impaired conditions of the monitored systems.
Frequency of occurrence:	Low, but at the moment it is not possible to associate past historical failures to specific cyber attacks.
Likelihood (probability) of success:	Medium (at least in the user agency due to the actual ICT network structure and topology)
Loss expectancy:	Should be low, but depends on the attacked IT service, its importance and the duration of the attack.
Consequences:	Legal exposure, economic loss, reputation loss, regulation

	compliance loss.
Compromised flow of events:	One or more threat agents target an ICT service through its devices that are somehow exposed (typically on the Internet); they could manage to reach the Core ICT Infrastructure network using one or more attack vectors / types (e.g. sending exploits to servers and communication devices, using DoS to silence the servers, use buffer overflows to subvert server services exposed, use fishing or spear fishing, etc.). One or more attacks complete successfully and the attacker possibly gains even more privileges or get a hold on other reachable assets. After a successful compromise, the attacked IT devices could: • Not operate the IT service any more. • Operate normal IT service and other not required. **Security (PANOPTESEC) Operations (MAPE cycle): [Monitor]** PANOPTESEC Security operators review alerts presented in the form of security status of the Monitored System (ICT environment). **[Analyze]** Security status indicators note the presence of one or more cyber incidents aligned with previously identified attack paths from hypothetical attack sources (both internal and external) to known mission critical systems. Potential impact on critical business functions (e.g., energy distribution) and non-critical business functions is assessed resulting in a quantified risk assessment. **[Plan]** Prioritized reactive mitigation actions are presented to the PANOPTESEC Security Operator. Reactive mitigation actions may consist of one or more discrete actions (e.g., exploited ports and protocols are blocked, exploited services are disabled). **[Execute]** Reactive mitigation actions are selected and executed by the PANOPTESEC Security Operators resulting in automated deployment where possible (e.g., firewall reconfigurations) or otherwise issuing instructions to Network and ICT Operators for follow-up deployment of mitigation actions (e.g., system reconfigurations outside PANOPTESEC Security Operator control). PANOPTESEC Security Operators also provide periodic status reports to Business Owners concerning the security status of their business (mission) operations. **Network and ICT Operations:** Network and ICT Operators receive notifications of mitigation actions from the PANOPTESEC Security Operators and take appropriate steps to implement the

	requested reactive mitigation actions. **Business Owners:** Business Owners receive periodic status reports concerning the security status of their business (mission) operations and provide oversight to ICT system operations.
Impact of compromise	Unavailability of the targeted business service due to loss of the relevant IT services. Possible legal and financial impacts arise as consequences of the loss of the IT services, mostly due to the loss of regulation compliance. For instance, Acea may be fined for outage of specific IT services.
Detection indicators:	Security alerts are logged by security software/devices (e.g., firewall logs, intrusion detection system alerts, anti-virus logs, connection logs, etc.) and PANOPTESEC system correlates them to on-going attacks.
Analysis indicators:	Possible attack paths should support PANOPTESEC Security Operators to understand if the actual situation is similar to an attack to the IT Service.
Valid mitigation options:	Notification and visibility of possible ongoing attacks are the top priority, but mitigation options could actually be available or not depending on the target(s). Depending the situation, valid mitigation actions may include, among others: • Patch deployment, system update; • Port and protocol reconfigurations; • Routing reconfigurations and/or ACL enabling/modifying; • Device quarantine.
Invalid mitigation options:	They depend on the attacked service and the nature of its nodes/devices.
Mitigation flow of events:	Mitigation actions are selected and executed by the PANOPTESEC Security Operator resulting in automated deployment of mitigation actions where possible (e.g., firewall

	reconfigurations) or otherwise issuing instructions to Network and ICT Operators for follow-up deployment of mitigations (e.g., system reconfigurations outside PANOPTESEC Security Operator control). PANOPTESEC Security Operators also provide periodic status reports to Business Owners concerning the security status of their business (mission) operations. **Network and ICT Operations**: Network and ICT Operators receive notifications of mitigation actions from the PANOPTESEC Security Operators and take appropriate steps to implement the requested security mitigation actions.
Post conditions:	After the application of the mitigation actions, the Network and ICT Operators regain control: all the previously affected systems are restored to proper operation and continue to maintain traces and audit logs.
Includes:	This macro-scenario is not referencing directly other scenarios, but can be specialized/customized obtaining more specific sub-scenarios (e.g. depending on the threat agents, attacks, number of assets compromised, duration of the attack, etc.) so it can be referenced.
Priority (define?):	Importance of scenario is Medium and the risk is acceptable depending on the role of the targeted ICT service and nodes. It should be present in the final list of demonstration scenarios.
Special requirements:	None.
Simulation Requirements:	The Simulation Environment must be able to properly emulate the existing ICT Services and provide appropriate sensors to support data collection requirements of the PANOPTESEC system.
Notes and Issues:	None.