FP7-610416-PANOPTESEC

Dynamic Risk Approaches for Automated Cyber Defence

D7.4.2 Demonstration System Prototype Report

Work-Package	WP7	Deliverable	D7.4.2
Due Date	31-10-2016	Submission Date	05-11-2016
Main Author(s)	RHEA		
Contributors	All project participants		
Version	V1.1	Status	Final
Dissemination Level	CO	Nature	PU
Keywords	Verification, Design, Requirements, Report, Operational Workshop		

Part of the Seventh

Framework Programme

Funded by the EC - DG Connect

EXECUTIVE SUMMARY

This document is a final report on Verification and Validation for the [D7.4.1], the Demonstration System Prototype for the PANOPTESEC System.

The whole Verification and Validation process is described and its results are presented.

In order to perform the Verification and Validation process, a methodology has been created and a web infrastructure (Redmine) has been configured in order to allow all work packages to centralise their collection of test cases and test executions.

In addition, a set of Demonstration Activities, with the aim of validate the PANOPTESEC prototype with internal (Acea representatives involved in the System Level Requirements definition) and external stakeholders have been conducted during Month 35 and 36.

The Verification process described in this document is the last step of the global PANOPTESEC Verification process, consisting on several iterations of design and requirements verification described within [D4.2.2R], [D5.2-3.3R], [D6.2.2R], [D7.2.2R], [D4.3.1R], [D5.4.1R], [D6.3.1R], [D7.3.1R], [D7.4.1R], [D8.2.2R].

In addition, this report includes information about performances of the PANOPTESEC System, Production Data tests, deployment of the PANOPTESEC System.

HISTORY

Version	Date	Name/Partner	Comment
V0.1	2016-10-10	Matteo Merialdo/RHEA	Initial creation of the document.
V0.2	2016-10-10	Matteo Merialdo/RHEA	Design Verification section added.
V0.3	2016-10-10	Matteo Merialdo/RHEA	Requirements Verification section added.
V0.4	2016-10-15	Matteo Merialdo/RHEA	Validation Section added
V0.5	2016-10-16	Matteo Merialdo/RHEA	Performance tests section added
V0.5	2016-10-16	Matteo Merialdo/RHEA	Production data tests section added
V0.6	2016-10-18	Matteo Merialdo/RHEA	Conclusions, annexes added
V0.6	2016-10-22	Herve Debar/IMT	QA Peer Review
V0.6	2016-10-22	Giuseppe Santucci/UNIROME	QA Peer Review
V0.7	2016-10-30	Matteo Merialdo/RHEA	Validation section added
V0.8	2016-11-01	Matteo Merialdo/RHEA	Validation section completed
V1.0	2016-11-04	Matteo Merialdo/RHEA	Document closed, comments from QA implemented
V1.1	2016-11-22	Matteo Merialdo/RHEA	Results from 5th October internal stakeholders workshop added

TABLE OF CONTENTS

TABLE OF FIGURES

LIST OF TABLES

ACRONYMS AND DEFINITIONS

Table 1: Acronym List

Acronym	Meaning
UzL	University of Lubeck
ACEA	ACEA S.p.A.
ALBLF	Alcatel-Lucent Bell Labs France
CIS-UROME	Universita Degli Studi Di Roma La Sapienza
EPIST	Epistematica SRL
IMT	Institut Mines-Telecom
RHEA	RHEA System S.A.
SUPELEC	Ecole Supérieure D'Électricité

Table 2: Definitions

Word or Phrase	Meaning
LLC	Low Level Correlator
MIM	Mission Impact Module
HLD	High Level Design
SNDA	Shallow Network Dependency Analyser
SNDM	Shallow Network Dependency Model
MG	Mission Graph
NI	Network Inventory
DCC	Data Collection Collector
DCI	Data Collection Interface
RMC	Reachability Matrix Correlator
AGG	Attack Graph Generator
HOC	High Level Online Correlator
PAI	Potential Attack Identifier
RQ	Risk Quantifier
SRD	Strategic Response Decider
TRD	Tactical Response Decider
PDP	Policy Deployer
ANM	Analysis Module
ASM	Actual Status Monitor
ARM	Attack Response Manager
TPM	Technical Project Manager
WP	Work Package

1 INTRODUCTION

1.1 Context

According to the Capability Maturity Model (CMMI-SW v1.1), it is possible to formally state the concepts of *Software Verification activity* and *Software Validation activity* as follows:

- The *Software Verification* is the process of evaluating software "to determine whether the products of a given development phase satisfy the requirements imposed at the start of that phase" [IEEE-STD-610]. In other words, Software Verification is the activity devoted to answering to the question "*Are we building the product right?"*
- The *Software Validation* is the process of evaluating software "during or at the end of the development process to determine whether it satisfies specified requirements" [IEEE-STD-610] and fits the intended use. In other words, Software Validation is the activity devoted to answering to the question "*Are we building the right product?*"

1.2 Purpose

The purpose of this report is to demonstrate that the [D7.4.1] software deliverable (*Demonstration System Prototype*) has been verified and validated by the consortium.

Verification activities take into consideration the set of requirements within [D2.2.1] deliverable, so system-level requirements (both functional and non-functional).

Validation activities, strengthened by the results of the tests over system-level requirements, consist of a set of complete demonstration activities (with final survey, directly traced to the System-level Requirements from [D2.2.1]) with internal stakeholders from the User Agency, the External Advisory Board and the consortium itself (Month 35). In addition, a second iteration of demonstration activities with external stakeholder is conducted during the last two weeks of Month 36 (with surveys).

Verification activities over [D7.4.1] have already been reported within [D7.4.1R], released at Month 34: this report presents another verification iteration (performed on Month 35) and gives additional details about the PANOPTESEC integrated prototype performance, production data tests and validation activities results.

1.3 Scope

The scope of this deliverable includes the verification and validation activities over the [D7.4.1] Deliverable, Demonstration System Prototype.

The presented verification activity is the fourth verification iteration over design, sub-system level requirements and system-level requirements held in March 2016, June 2016, August 2016 and September 2016. These verification activities have been already reported within [D4.2.2R], [D5.2-3.3R], [D6.2.2R], [D7.2.2R], [D4.3.1R], [D5.4.1R], [D6.3.1R], [D7.3.1R], [D7.4.1R], [D8.2.2R].

Document Structure

This [D7.4.2] 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.

Section 3 PANOPTESEC System Design Verification: assesses the verification of the PANOPTESEC System Design with respect to the HLD of [D3.1.2] and the updates reported in [D4.2.2R], [D5.2-3.3R], [D6.2.2R], [D7.2.2R], [D4.3.1R], [D5.4.1R], [D6.3.1R], [D7.3.1R], [D7.4.1R], [D8.2.2R].

Section 4 PANOPTESEC System Requirements Verification: documents the verification and validation process of PANOPTESEC System related requirements towards identified requirements in [D2.2.1], in [D4.1.1], [D5.1.1] and [D6.1.1].

Section 5 PANOPTESEC System Components Integration Verification: describes how the Integration Tests have been performed.

Section 6 PANOPTESEC System Validation activities: describes the Validation activities over the PANOPTESEC Prototype, encompassing live demonstrations with internal and external stakeholders.

Section 7 PANOPTESEC System deployment: describes the final deployment of the PANOPTESEC System.

Section 8 PANOPTESEC System performances results: after several months of tests and several improvements on the source code and the orchestration, it is possible to summarize the final results of the PANOPTESEC System in terms of performances.

Section 9 PANOPTESEC System production data tests: the PANOPTESEC System has been developed with masked production data and emulation environment data and verified with emulation environment data (the emulation environment, validated by the User Agency as an operational environment, has a very high affinity with the production environment which it is replicating). In order to demonstrate that the PANOPTESEC System is also able to work on a production environment, a set of tests have been performed and their results are presented in this section.

Section 10 Conclusion: summarizes the findings, results and recommendations.

2 METHODOLOGY

2.1 Verification Methodology

This section details the verification methodology followed by the PANOPTESEC consortium in order to prove that software released in [D7.4.1] and updated within Month 35 covers the specifications.

The consortium conducted four verification iterations over the software, at Month 28, Month 32, Month 34 and Month 35. Tests have been repeated on all cases in which a change has been recorded, in order to ensure non-regression. For example, since several components have been closed at Month 32, their tests have not been repeated on Month 34 and 35.

Already used for tracking bugs during the development of the PANOPTESEC system, the Redmine online platform (https://panoptesec.isp.uni-luebeck.de/) has been properly adapted and used to record all details of the verification process.

Our verification process is performed in 3 steps:

1. *Requirements and design review*: during every software project lifecycle, it is common to have requirement changes and/or updates in the design due to the always-increasing understanding of the functionalities and their challenges. As a consequence, a fundamental step before proceeding in the "real" software verification is the assessment of the functional and non-functional requirements and the system design.
2. *Test Cases definition*: once requirements and design are assessed, it is possible to proceed with the definition of test cases whose aim is to verify the software conformance with respect to (i) its functional specification following from functional requirements and (ii) its deployment and any other non-functional aspect following from non-functional requirements and design choices.
3. *Test Execution*: every defined test case is finally executed to verify the conformance of the actual results with respect to the expected ones.

2.1.1 Information collection

Concerning phase 1 (Requirement and design review), we started the review process on Month 28 by analyzing all the requirements related to the release [D7.4.1] and traced in the SysML project encompassing high-level designs, low-level designs and requirements modelling (the design projects have been released within the [D7.4.1]). The final aim of this phase is a list of requirement actions requests to update, delete or create requirements. During the first iteration of the process, at Month 28, several detailed requirements have been identified as obsolete, but no change requests were submitted. During Month 30, following the Change Request methodology described in [PH15], all obsolete requirements have been officially labelled as obsolete, a rationale has been included to describe the reasons for obsolescence, and they will not sustain a verification process. In [D4.2.2R], [D5.2-3.3R] and [D6.2.2R] all rationale over obsolete requirements have been given and

validated during the 4th Project Review that occurred 22 April 2016. All obsolete requirements have been summarized within [D4.3.1R], [D5.4.1R], [D6.3.1R].

Within [D4.3.1], [D5.4.1], [D6.3.1] and [D7.3.1] all remaining detailed requirements from [D4.1.1], [D5.1.1] and [D6.1.1] have been verified during the second verification iteration performed at Month 32.

A second action item of the review process is the analysis of the High-Level Design (HLD) described in [D3.1.2]. The High-Level Design of the PANOPTESEC System is kept up-to-date by Work Package 7 during the whole implementation phase: all requested changes have been analysed in order to ensure that no deviations, possibly compromising the capabilities of the system, occur. As it is common in every software project, the High-Level Design of the PANOPTESEC System changed on several details during the implementation phase. It is then important that all these changes are considered in terms of impact on the desired functionalities (depicted in the Requirements). The Verification process (Phase 2 and 3) will then show that the current and final implementation of the components covers the identified Requirements despite the changes.

In order to ensure that the software implementation under analysis verifies the actual High Level Design, a special set of test cases (conducted mainly with code and interfaces inspection) must be created and conducted.

Concerning phase 2 (Test Cases definition), at least one test case MUST be defined for each requirement related to the [D7.4.1] release.

NOTE: With the term 'test case ' we denote the "abstract" description of the test case and we consider the possibility to define both *human tests* (i.e., code inspection, design inspection etc.…) and *computer-based tests* (i.e., component test, integration test etc.…).

Unfortunately, when checking the functional coverage against requirements, there is not a unique and general methodology to define test cases as they depend on the specific requirement. In the following, we will describe the general working pattern followed in our verification process.

Concerning Functional requirements, the following checks should be included in each test case:

1. **"Syntactic" functionality check**: the aim of this check is to answer to the question "Is there an evidence in the project (code/ design/ etc…) that the functionality can be supported?"
   As an example, let us consider the following requirement:

   WP5.HOC.R8 "*The HOC module must be able to automatically transform attack graphs into correlation rules that can be handled by the module itself".*

   It implies the definition of one or more functions able to take as input an attack graph and to generate, as output, a set of correlation rules.

The test case must check and identify a piece of software (e.g. a method, a class, etc.…) implementing such functionality. In the case of QBE-HOC, this functionality is implemented by the method newQueryTranslation() in the class QueryTranslation.

2. **"Semantic" functional check**: If the "syntactic" check succeed and identifies the set of classes/methods etc.… implementing the needed functionality, the "semantic" check has the aim to verify that the corresponding implementation is correct with respect to its semantic (i.e., the software behaves as it is supposed to do for the given inputs). This can be done in different ways depending on the specific requirement (e.g., by using black box testing on the subset of identified methods/classes and comparing expected input/output pairs with actual input/output pairs). Input should be selected in order to test valid values, invalid values, boundary conditions, exceptional cases etc.

   Taking again example of the requirement WP5.HOC.R8, the test case must check that the implementation of the method newQueryTranslation() offered by QBE takes as input an EAG object and produces as output a list of EPL queries. This check is basically the *acceptance criteria* that will allow assessing the coverage of the requirement.
   Therefore, it is fundamental that this check is clearly defined and expressed.

3. **Effectiveness functional check**: this check is optional. Its aim is to verify the "goodness" of the implementation with respect to previously specified effectiveness parameters. Let us note that, this check has meaning usually only for functionalities implemented trough non-deterministic algorithms (e.g. approximated algorithms or random-based algorithms). In this case, the test definition depends on the nature of the implementation and can be different case by case.

Check 1 and 2 are mandatory for each functional requirement while check 3 should be done when needed.

For the sake of completeness, the template for the definition of our test cases (and the meaning of each field) is provided in the following table. The same template is imported in Redmine (https://panoptesec.isp.uni-luebeck.de/) where all the test cases have been loaded.

Project Name: PANOPTESEC	
Test Case Template for Functional Requirement	
General Information	
Test Case ID:	<Unique test case identifier>
Test Designed by:	<Member of the consortium that defined the test case>
Requirement ID:	<Identifier of the test case that can be assed trough the execution of this test case>
Objective:	<Text explaining the objective of the requirement>
Syntactic Test	
Basic Functions needed to satisfy the requirement:	<Description of the basic functionalities or design patterns that should be implemented to support the coverage of the requirement>
Are such Functions implemented by a piece of software or granted by design?	<(Y/N)>
List the sources allowing to verify the coverage (e.g., diagram, classes/functions/methods involved in the implementation)	<List the sources of evidence that allows to verify that basic functionalities or design patterns exists in the project>
Semantic Test	
Component(s):	<(List of) Component(s) implementing the functionalities or the design pattern identified in the syntactic part>
Acceptance Criteria:	<A clear condition on the input/output that allows to assess the correctness of the actual behaviour with respect to the expected one>
Verification Method:	<Selection among few possible options>
Pre-conditions:	<(List of) Condition(s) that should be true in order to execute the test case>
Dependencies:	<(List of) External source(s) needed to execute the test case>
Post-conditions:	<(List of) Condition(s) that should be true at the end of the test case execution>
Effectiveness Test	
Given the input data, is the output data deterministic?	<(Y/N)>
Effectiveness parameter(s) and corresponding assessment method(s)	<(List of) Parameter(s) that should be evaluated to assess the goodness of the current implementation>

An example of filled test case to verify WP5.HOC.R8 requirement is reported in the following table.

Project Name: PANOPTESEC	
Test Case Template for Functional Requirement	
General Information	
Test Case ID:	TC.WP5.HOC.R8
Test Designed by:	UROME
Requirement ID:	WP5.HOC.R8
Objective:	The module MUST be able to automatically transform the information provided by AGG into correlation rules representing a format usable by the HoC.
Syntactic Test	
Basic Functions needed to satisfy the requirement:	A method (*queryTranslation*) that takes in input the Attack Graph, and for every event of this one, it produces the corresponding query, useful for the component.
Are such Functions implemented by a piece of software or granted by design (Y/N)?	Y
List the sources allowing to verify the coverage (e.g., diagram, classes/functions/methods involved in the implementation)	QueryTranslation class, queryTranslation() method.
Semantic Test	
Component(s):	QBE-HOC
Acceptance Criteria:	The test is accepted if, given an attack graph provided by AGG, the newQueryTranslation() method generates the set of strings corresponding to EPL queries for the following statement: for every event (leaf of Attack Graph) we have a query able to detect alerts with the same ingress address, egress address and CVE pairwise.
Verification Method:	software component test
Pre-conditions:	NA
Dependencies:	NA
Post-conditions:	NA
Effectiveness Test	
Given the input data, is the output data deterministic?	Y
Effectiveness parameter(s) and corresponding assessment method(s)	NA

Non-functional requirements are usually specified at the component level and are verified at component level.

Unfortunately, in this case there is no standard way to proceed as the test case will depend on the requirement. We will provide some example as guidelines.

Example 1: Let us consider requirement WP5.HOC.R16 in D5.1.1: "*The module SHOULD ensure the security of raised high level alerts*". In this case, the test is simply done by code inspection verifying if the appropriate cryptographic mechanism has been put in place.

Example 2: Let us consider requirement WP5.HOC.R16 in D5.1.1: "*The HOC module SHOULD automatically be able to scale in terms of incoming low-level alerts rate*". In this case, we need to evaluate scalability by changing the low-level alert rate. Thus, we first need to specify which are the metrics that should be able to scale (e.g., CPU usage, Memory space) and then run different simulation where the only difference is the input rate. The result of the test is a qualitative trend of the behaviour of the component and is represented in a graphic.

To specify these test cases, we re-use the same template provided so far. Note that for non-functional requirements, not all the entries could be filled.

The resulting tables follow:

Project Name: PANOPTESEC	
Test Case Template for Non-Functional Requirement	
General Information	
Test Case ID:	TC.WP5.HOC.R16
Test Designed by:	UROME
Requirement ID:	WP5.HOC.R16
Objective:	The module SHOULD ensure the security of raised high level alerts
Syntactic Test	
Basic Functions needed to satisfy the requirement:	Availability of cryptographic functions/libraries to encrypt/sign alerts before propagation.
Are such Functions implemented by a piece of software or granted by design (Y/N)?	N
List the sources allowing to verify the coverage (e.g., diagram, classes/functions/methods involved in the implementation)	NA
Semantic Test	

Component(s):	QBE-HOC
Acceptance Criteria:	The test is accepted if it is possible to show that the module encrypts or digitally signs every high-level alert.
Verification Method:	code Inspection
Pre-conditions:	NA
Dependencies:	NA
Post-conditions:	NA
Effectiveness Test	
Given the input data, is the output data deterministic?	NA
Effectiveness parameter(s) and corresponding assessment method(s)	NA

Project Name: PANOPTESEC	
Test Case Template for Non-Functional Requirement	
General Information	
Test Case ID:	TC.WP5.HOC.R15.1
Test Designed by:	UROME
Requirement ID:	WP5.HOC.R15
Objective:	The HOC module SHOULD automatically be able to scale in terms of incoming low-level alerts rate
Syntactic Test	
Basic Functions needed to satisfy the requirement:	Optimized memory management and basic functions implemented trough efficient algorithms
Are such Functions implemented by a piece of software or granted by design (Y/N)?	Y
List the sources allowing to verify the coverage (e.g., diagram, classes/functions/methods involved in the implementation)	eu.panoptesec.querybasedengine.* package
Semantic Test	
Component(s):	QBE-HOC
Acceptance Criteria:	The test case is accepted if a set of Pictures is provided showing how performance of the module (CPU and Memory Usage) degrades (or gracefully degrade) when LLCAlert arrival rate increases.
Verification Method: <selection among few possible options>	Component Test
Pre-conditions:	NA
Dependencies:	NA

Post-conditions:	NA
Effectiveness Test	
Given the input data, is the output data deterministic?	N
Effectiveness parameter(s) and corresponding assessment method(s)	CPU consumption and memory consumption. The CPU consumption is based on the size of the incoming LLCAlerts queue. Monitoring such parameter while varying the LLCAlert arrival rate should assess the degradation.

NOTE: the naming convention for the field "Test Case ID" is as follows: "TC.<ReqId>". If more than one test case is defined for the same requirement a sequence number should be added to the test case id (e.g., "TC.WP5.HOC.Rx.1", "TC.WP5.HOC.Rx.2", "TC.MIM001", "TC.MNT001-MNT002.1" etc…).

A tutorial wiki guide has been created to support the use of Redmine in the test case definition process and it is available on line at the following link: https://panoptesec.isp.uni-luebeck.de/projects/wp4/wiki.

Concerning phase 3 (Test Execution), test cases defined so far must be implemented trough one or more *test executions* i.e., a concrete instance of the test specified by the test case.

In other words, a test execution specifies a tuple <input, expected output, actual output>.

As an example we show a test execution template (in a tabular form):

Test	Test Input Data	Expected Result	Actual Result	Status (Pass/Fail)	Notes	Test Executed by:	Test Execution date:
TC-HOC-x.y		<Reference to output file>	<Reference to output file>	Pass		UROME	07/01/2016

Also in this case, the template provided is imported in Redmine (https://panoptesec.isp.uni-luebeck.de/) where all the test executions have been loaded.

Each partner in the consortium has been responsible for executing and reporting of its test cases (i.e., the ones identified in the previous steps).

JUNIT tests are recommended (for JAVA based components) as they can be re-used later on in further cycles of testing to ensure non-regression. However, the testing methods are up to the testers.

From a practical point of view, several best practices have been adopted in defining test executions:

- Decompose a coarse-grained functionality into fine-grained ones, define basic test cases for fine-grained functionalities and then assess the coarse-grained functionality consequently.

- Define synthetic and small input data in order to compute the expected output by hand.
- Use firstly deterministic input data (this is especially true for reactive components that are subjects to errors).
- **RECALL**: Reactive Components should also consider testing the behaviour of the component with non-deterministic input data set (i.e., same data received in a different order, missing data, etc.). In this case, the same tests should be repeated more than once in order to make it significant and the report should be the aggregation of the different execution.

2.1.2 Information analysis

In order to assess the coverage of each requirement, the consortium extracted the lists of test cases and related executions from Redmine and evaluated whether or not the outcome of the executions guarantees the coverage of each requirement (partially or globally). A synthesis of the results is shown in Section 4.

In order to ensure a good quality of the produced test cases and test executions and in order to assess the final results of the process, a verification team has been selected from the consortium members. Each test case and each test execution have been then reviewed and, if necessary, commented. It was then of course up to the tester to implement the comments. The verification team also assisted the consortium on every step of the process.

2.2 Validation Methodology

2.2.1 Information collection

After the installation of the PANOPTESEC System [D7.4.1] (described in Section 7), the system is ready for presentation during the live workshops, whose structure and flow is described within [D8.2.1]. These workshops are composed of several demonstration activities, designed in order to be able to cover all system-level requirements. This allows the involved stakeholder (internal or external) to validate all the functionalities of the PANOPTESEC system and give an overall evaluation of the results of the Project.

The consortium organized 3 workshops with internal stakeholders (User Agency representatives and External Advisory Board members, involved in the requirements gathering phase described within [D2.2.1] in order to collect their feedbacks. Each workshop lasted from 3 to 6 hours, in order to give the stakeholders the opportunity of exploring the PANOPTESEC system prototype with a high level of detail. Results from these demonstrations have been documented in [D8.2.2] and have been examined during the Qualification Review performed on October 11th 2016.

The consortium organized then 18 workshop sessions with external stakeholders in order to receive a final feedback from a larger community. Also in these cases, each demonstration activity lasted from 2 to 5 hours, with the aim of showing the PANOPTESEC System with the greater possible level of detail and analyse step by step each of the Demonstration Activities defined within [D821] (with the final aim of validating the traced system-level requirements).

As a result from the live demonstrations, the consortium collected answers to a feedback questionnaire (on paper), given to all attendees.

The survey follows the storyline of the Workshops, as it has been described within [D8.2.1]. Each workshop is divided into Demonstration Activities (DA), which cover the validation of the system-level requirements from [D2.2.1]. For each DA, a specific set of questions is proposed. Additional, more general questions are then asked as a summary for the session.

Each question was given a rank between 0 and 5 following the scale:

- 0: not able to answer
- 1: very poor/no
- 2: poor
- 3: sufficient
- 4: good
- 5: very good/yes

The questionnaire is reported in Table 3:

Table 3: Operational Workshops questionnaire

Operational Workshop	
Date	
Surname	
Name	
Company	
Role	
email	

	0: not applicable 1:very poor/no 2: poor 3: sufficient 4: good 5:very good/yes						
DA01	**Monitored System Overview**						
1.1	Does the System show a correct network, topology and system inventory (comprehensive asset identification) ?	0	1	2	3	4	5
1.2	Is the network, topology and system inventory appropriate for the project's goals?	0	1	2	3	4	5
1.3	Is the network reconstruction showing useful geographical information?	0	1	2	3	4	5
DA02	**Monitored System Vulnerability Surface**						
2.1	Does the System show a correct vulnerability inventory (correlation of assets to known vulnerabilities) ?	0	1	2	3	4	5
2.2	Is the vulnerability inventory appropriate for the project's goals?	0	1	2	3	4	5
DA03	**Monitored System Mission Impact assessment**						
3.1	Does the System show a correct view of the business processes of the Company, correlated with the dependent ICT/SCADA devices?	0	1	2	3	4	5
3.2	Is the view of the business processes and their relationship with the ICT/SCADA device appropriate for the project's goals?	0	1	2	3	4	5
DA04	**Risk Analysis, Proactive Risk and Attack Graph**						
4.1	Does the System show a correct detection of the possible attack paths within the Monitored System, given a set of entry points?	0	1	2	3	4	5
4.2	Is the attack paths detection consistent with the network topology reconstruction?	0	1	2	3	4	5
4.3	Is the attack paths detection useful?	0	1	2	3	4	5
4.4	Does the System show a reconstruction of the quantification of the level of the Risk of the System?	0	1	2	3	4	5
4.5	Is the Risk quantification analysis appropriate for the project's goals?	0	1	2	3	4	5
DA05	**Strategic Response Overview**						
5.1	Does the System show a prioritized strategic dashboard, with related strategic response plans optimized by risk reduction, response on financial investment impact evaluation and operational impact evaluation?	0	1	2	3	4	5
5.2	Is the strategic response plan computation consistent with the topology of the Monitored System and the quantification of the actual level of the Risk?	0	1	2	3	4	5
5.3	Is the strategic dashboard useful?	0	1	2	3	4	5
DA06	**Architecture Component Overview**						

6.1	Is the software architecture of the Panoptesec coherent with the purposes of the Project?	0	1	2	3	4	5
6.2	Are the Panoptesec software security mechanisms (authentication, crtiptography, etc.) providing an adequate protection for sensitive data?	0	1	2	3	4	5
DA07	**Incident Correlation Overview (IAP analysis)**						
7.1	Is the System able to correlate perceived security incidents with the computed attack paths?	0	1	2	3	4	5
7.2	Does the System visualize these correlation in order to alert the operator that a an attack is ongoing?	0	1	2	3	4	5
7.3	Is the System able to quantify the reactive level of the Risk, given a set of correlated incidents?	0	1	2	3	4	5
DA08	**Tactical Response Plan**						
8.1	Does the System show a prioritize reactive dashboard, with related tactical response plans optimized by risk reduction and operational impact evaluation?	0	1	2	3	4	5
8.2	Are the tactical response plans coherent with the perceived correlated incidents?	0	1	2	3	4	5
8.3	Is the tactical dashboard useful?	0	1	2	3	4	5
Q01	**Do you think that the attack scenarios are realistic?**	0	1	2	3	4	5
Q02	**Do you think that the Panoptesec response time from a proactive perspective is appropriate?**	0	1	2	3	4	5
Q03	**Do you think that the Panoptesec response time from a reactive perspective is appropriate?**	0	1	2	3	4	5
Q04	**Is the graphical user interface appropriate for the project's goals?**	0	1	2	3	4	5
Q05	**Do you think that the Panoptesec or some part of the Panoptesec could be useful in your organization?**	0	1	2	3	4	5
Q06	**Does the system provide useful information?**	0	1	2	3	4	5
Q07	**Does the system provide up to date information?**	0	1	2	3	4	5
Q08	**Is the information clear?**	0	1	2	3	4	5
Q09	**Is the system easy to use?**	0	1	2	3	4	5
Comments:							

2.2.2 Information analysis

The results have been commented between the partners during the Qualification Review (11th of October) and during the Acceptance Review (November 2016).

2.3 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) established by a QAM, validated at a consortium level and centralized in the Project Handbook [PH15].

For the purpose of the QA of the [D7.4.2] report, the deliverable MUST be assessed according the following checklists:

- PEER REVIEW (PR) QA CHECKLIST: the [D7.4.2R] deliverable is a report; it then requires a proper peer review.

3 PANOPTESEC SYSTEM DESIGN VERIFICATION

3.1 Introduction

Deliverable [D3.1.2] (System High Level Design) encompassed the overall High Level Design of the PANOPTESEC System.

The PANOPTESEC System is composed of several set of components, collected within sub-systems and developed within different Work Packages. In addition, Work Package 7 developed and Integration Framework with the main tasks of integrating all components and manage the orchestration, the runtime management, the messaging system and the possible connections with other systems/components.

Deliverable [D4.2.2R] and then [D4.3.1R], related to the Data Collection and Correlation subsystem detailed and justified the differences between the Design described in [D3.1.2] and the Design at 29 February 2016 and then 17 June 2016. The current design (23 September 2016), does not deviate from the [D4.3.1R] version.

Deliverable [D5.2-3.3R] and then [D5.4.1R], related to the Dynamic Risk Management Response subsystem detailed and justified the differences between the design described in [D3.1.2] and the design at 29 February 2016 and then 17 June 2016. The current design (23 September 2016), does not deviate from the [D5.4.1R] version.

Deliverable [D6.2.2R] and then [D6.3.1R], related to the Visualization subsystem detailed and justified the differences between the Design described in [D3.1.2] and the Design at 29 February 2016 and then 17 June 2016. The current design (23 September 2016), does not deviate from the [D6.3.1R] version.

Deliverable [D7.2.2R], then [D7.3.1R] and then [D7.4.1R] detailed and justified the differences between the overall PANOPTESEC System Design described in [D3.1.2] and the design at 29 February 2016, then 17 June 2016 and then 19 August 2016. The current design (23 September 2016), does not deviate from the [D7.4.1R] version.

Please note that this is not intended as a Design Deliverable but as a report of design updates and verification of the developed software.

A summary of the current High Level Design is in Annex A, while the complete High Level and Low Level designs, in terms of extracted images and SysML/UML Papyrus projects can be found within the [D7.4.1] package.

3.1.1 PANOPTESEC System

The PANOPTESEC System is presented in [D3.1.2], Section 5.2.

The current implementation of the PANOPTESEC system deviates from the high level architecture presented in [D3.1.2], Section 5.2: all updates in the design have been presented, justified and verified within [D4.2.2R], [D4.3.1R], [D5.2-3.3R], [D5.4.1R], [D6.2.2R], [D7.2.2R] and [D7.3.1R].

In this Section it is verified if the PANOPTESEC System implementation is still representative of the architecture presented in [D3.1.2] and updated within the development phase. In addition, in order to show that with the current stable version (23 September 2016) the integration phase is completed, Sequence Diagrams from the Low Level Design, encompassing complex orchestrations between integrated components will be verified in order to show that the developed software is compliant with the designed behavior.

3.2 Design Verification

In order to fill the gap between the High Level Design and the code implementation, a Low Level Design, focused on integration, messaging and interfaces, has been developed. It directly derives from the High Level Design (the two Designs, linked by traceability links, are available within the Papyrus Project part of the [D7.4.1]).

All Design Test Cases and the corresponding Test Executions can be found within the Design Project in the Redmine website (https://panoptesec.isp.uni-luebeck.de/projects/design).

In the following, we will provide a schematic summary of the Design Verification extracted from the Redmine website. The colour coding convention used is reported in Table 4.

3.2.1 Caption

Color	TC Exists?	TE Exists?	Outcome	Redmine Documentation Status
	N	N	N	
	Y	N	N	In Progress

	Y	Y	N (all TEs fail)	Rejected
	Y	Y	Partial (not 100% TEs succeeds)	In Progress
	Y	Y	Y	Resolved

Table 4 – Color Coding Used for the final assessment of Design Verification

Most of tests have been conducted by code inspection, with the aim to show that the components correctly implement the defined interfaces. For the Integration Framework, however, complex integration tests are conducted in order to show the coverage of the so far integrated system with the orchestration in the Sequence Diagrams depicted in [D7.4.1].

3.2.2 Data Collection Interface package Design Verification

ID	Test Case ID	Component(s)
DCI-VAC	TC.DCI-VAC.1	VulnerabilityAdvisoryCollector / VulnerabilityAdvisoryCollectorBundle
DCI-DACPC	TC.DCI-DACPC.1	DeployedAccessControlPolicyCollector / VulnerabilityAdvisoryCollectorBundle
DCI-BMC	TC.DCI-BMC.1	BusinessMissionCollector
DCI-NDA	TC.DCI-NDA.1	NetworkDependencyAnalyser / NetworkDependencyAnalyserBundle

3.2.3 Data Collection Collector package Design Verification

ID	Test Case ID	Component(s)
DCC-NIP	TC.DCC-NIP.1	NetworkInventoryProcessor / NetworkInventoryProcessorBundle
DCC-VIP	TC.DCC-VIP.1	VulnerabilityInventoryProcessor / VulnerabilityInventoryProcessorBundle
DCC-PM	TC.DCC-PM.1	PersistencyManager / PersistencyManagerBundle

3.2.4 Low Level Correlator package Design Verification

ID	Test Case ID	Component(s)
LLC	TC.LLC.1	LowLevelCorrelator / LowLevelCorrelatorBundle

3.2.5 Reachability Matrix Correlator package Design Verification

ID	Test Case ID	Component(s)
RMC	TC.RMC.1	ReachabilityMatrixCorrelator / ReachabilityMatrixCorrelatorBundle

3.2.6 Mission Impact Module package Design Verification

ID	Test Case ID	Component(s)
MIM	TC.MIM.1	MissionImpactModule / MissionImpactModuleBundle

3.2.7 AttackGraphGenerator-ThreatRiskQuantifier package Design Verification

ID	Test Case ID	Component(s)
AGG-TRQ	TC.AGG-TRQ.1	AGG-TRQ / AGG-TRQBundle

3.2.8 StrategicResponseDecider package Design Verification

ID	Test Case ID	Component(s)
SRD	TC.SRD.1	StrategicResponseDecider / StrategicResponseDeciderProxy

3.2.9 High level online Correlator package Design Verification

ID	Test Case ID	Component(s)
HOC-QBE	TC.HOC-QBE.1	QueryBasedEngine / QueryBasedEngine Bundle
HOC-ABE	TC.HOC-ABE.1	AutomataBasedEngine / AutomataBasedEngine Bundle
HOC-PAI		PotentialAttackIdentifier

3.2.10 TacticalResponseDecider package Design Verification

ID	Test Case ID	Component(s)
TRD	TC.TRD.1	TacticalResponseDecider / TacticalResponseDeciderBundle

3.2.1 Visualization System package Design Verification

ID	Test Case ID	Component(s)
VIZ	TC.VIZ.1	Visualization / VisualizationProxy

3.2.2 Integration Framework Design Verification

ID	Test Case ID	Component(s)
IF	TC.IF.1	Integration Framework
	TC.IF.2	
	TC.IF.3	
	TC.IF.4	
	TC.IF.5	

The PANOPTESEC system is still completely integrated as for the 23 September 2016 Version of the system.

3.2.3 Policy Deployer Design Verification

ID	Test Case ID	Component(s)
PD	TC.PD.1	PolicyDeployer / PolicyDeployer Bundle

3.2.4 Conclusions

After the analysis over the actual High Level Design and its implementation, it is possible to say that the Design, in terms of input/output interfaces, is completely verified, with the only exception of the PAI component (currently, it is not developed and a rationale for this choice has already been provided in [D5.2-3.3R].

In terms of integration dependencies and verification of the orchestration defined in the design via Sequence Diagrams and Activity Diagrams, the Integration Framework, the Policy Deployer, the Data Collection and Correlation subsystem, the Dynamic Risk Management Response subsystem and the Visualization system have been fully verified.

4 PANOPTESEC SYSTEM REQUIREMENTS VERIFICATION

4.1 Introduction

The PANOPTESEC consortium identified specific requirements for the PANOPTESEC System within [D2.2.1], both Functional and Non-Functional. This report, describing the Verification and Validation process over the Demonstration System Prototype [D7.4.1], focuses on these System Level Requirements. Deliverables [D4.3.1R], [D5.4.1R] and [D6.3.1R] reported the verification results over all detailed Requirements *refining* System Level Requirements: this *refine* notation connecting detailed Requirements to System Level Requirements allows to already assess an initial coverage and verification for them. Within [D7.4.1R] a first complete, detailed, analysis over [D2.2.1] Functional and Non-Functional Requirements has been made.

This deliverable proposes the latest, updated, version of the Verification activities (as can be seen, some slight updates occurred from the [D741R]) over all PANOPTESEC System Requirements: after the release of [D741] on Month 34, a last major release of the software have been versioned the 23 September 2016 (Verification Report is in [D822R]) and some small minor updates have been performed until 16 October 2016 in order to cover the last non verified Requirements.

In [D2.2.1] section on the Redmine website (as explained in Section 2) it is possible to find all considered Functional and Non-Functional Requirements, their Test Cases and Test Executions. This report collects the results (in terms of requirements verified, not verified and partially verified) from the Redmine tool.

This report also summarises the verification results of the PANOPTESEC sub-systems over the detailed Requirements as reported within [D4.3.1R], [D5.4.1R] and [D6.3.1R] within Annex B.

During the first iteration of the process, at Month 28, some detailed requirements from [D4.1.1], [D5.1.1] and [D6.1.1] have been identified as obsolete, but no change requests were submitted. During month 30, following the Change Request methodology described in [PH15] (Configuration Management procedures, Section 3.3), all obsolete requirements have been officially defined as obsolete and they will not sustain a verification process. In [D7.2.2R] all rationale over obsolete requirements have been given and validated during the 4th Project Review in 22 April 2016. All obsolete Requirements and their rational can be found within [D4.3.1R], [D5.4.1R] and [D6.3.1R].

In the following, we will provide a schematic summary of the Requirement Verification results extracted from the Redmine website (in terms of requirements verified and not verified). The colour coding convention used is reported in Table 5.

4.2 Caption

Colour	TC Exists ?	TE Exists?	Deprecated Requirement (will never fulfilled, yet a TC must exist)	Outcome	Redmine Requirement Status
	N	N	N	N	
	Y	N	Y	N	Closed
	Y	N	N	N	In Progress
	Y	Y	N	N (all TEs fail)	Rejected
	Y	Y	N	Partial (not 100% TEs succeeds)	In Progress
	Y	Y	N	Y	Resolved

Table 5 - Color Coding used for the final assessment of Requirement coverag

4.3 Non-Functional Requirements

4.3.1 Compatibility Requirements Verification

ID	Description	Importance	Test Case ID	Component(s)
CMP001	The PANOPTESEC System MUST be modular and decomposed in different components in order to improve flexibility (in organization and configuration), ability to develop new function combinations rapidly and component re-use	3	TC.CMP001.1	Integration_Framework
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.	3	TC.CMP002.1 TC.CMP002.2 TC.CMP002.3 TC.CMP002.4	Integration_Framework
CMP003	Functional components SHOULD access to collected data in a transparent way to reduce complexity for developers.	2	TC.CMP003.1	Integration_Framework, PersistencyManagerBundle
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)	2	TC.CMP004.1 TC.CMP004.2 TC.CMP004.3 TC.CMP004.4	Integration_Framework
CMP005	The PANOPTESEC system MUST accept alerts in IDMEF format.	3	TC.CMP005.1	LowLevelCorrelator
CMP006	To cope with IDS that would not produce alerts in IDMEF, a translator to IDMEF SHOULD be provided.	2	TC.CMP006.1	LowLevelCorrelator
CMP007	It SHOULD be possible to deploy the various functional components of the PANOPTESEC system on the same physical machine or on different machines.	2	TC.CMP007.1	Integration_Framework

CMP008	It SHOULD be possible for a system administrator to manage the runtime of each single component of the PANOPTESEC System.	2	TC.CMP008.1	Integration_Framework
CMP009	XML and JSON SHOULD be used as formats for data object exchanges.	2	TC.CMP009.1	PANOPTESEC Data Model

4.3.2 Maintainability Requirements Verification

ID	Description	Importance	Test Case ID	Component(s)
MNT001	The PANOPTESEC System MUST be modular and decomposed in different components in order to improve maintainability.	3	TC.MNT001.1	Integration_Framework
MNT002	The PANOPTESEC data model SHOULD be designed to support integration with new data sources in the monitored system(s)	2	TC.MNT002.1	PANOPTESEC Data Model
MNT003	The PANOPTESEC System SHOULD provide a unique configuration environment to ease the maintenance of the deployed components.	2	TC.MNT003.1	Integration_Framework
MNT004	The PANOPTESEC System SHOULD be comprised of a fully integrated system of functions from detection to automated response recommendation and actuation.	2	TC.MNT004.1	PANOPTESEC System

4.3.3 Performance Requirements Verification

ID	Description	Importance	Test Case ID	Component(s)
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.	2	TC.PRF001.1 TC.PRF001.2 TC.PRF001.3 TC.PRF001.4 TC.PRF001.5	PANOPTESEC System
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.	2	TC.PRF002.1	PANOPTESEC System
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.	2	TC.PRF003.1 TC.PRF003.2	PANOPTESEC System
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.	2	TC.PRF004.1	PANOPTESEC System
PRF005	The PANOPTESEC components SHOULD be able to each run in a 32GB dual core 2Ghz Virtual machine.	2	TC.PRF005.1	PANOPTESEC System / Integration_Framework
PRF006	The PANOPTESEC system SHOULD reduce Security Operator response time from hours to seconds in response to identified cyber incidents.	2	TC.PRF006.1	PANOPTESEC System
PRF007	The PANOPTESEC System SHOULD reduce operator analysis of security status from days to minutes.	2	TC.PRF007.1	PANOPTESEC System
PRF008	The PANOPTESEC System MUST propose only approved course of actions responses that do not adversely affect operations.	3	TC.PRF008.1 TC.PRF008.2	PANOPTESEC System

Summary and rationale of non-verified requirements:

Requirement			Motivation	Expected Impact
ID	Description	I		
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.	2	It is not possible to quantify all the possible False Negatives occurring in the monitored system even if it has a defined attack surface. It is possible to say that since the PANOPTESEC system works at a higher level with respect to the monitored system sensors (IDS, Firewall), hence it contributes to the detection of false negatives. An example of this is explained in https://panoptesec.isp.uni-luebeck.de/issues/5014 where the detection of an event by the system sensors does not occur and where we can observe if a path that includes an edge relative to the malicious event is instantiated, and therefore it is take into account by other PANOPTESEC components. However, since it is not possible to quantify the initial set over which we can perform our analysis, it is also not possible to quantify the false negative reduction and say that this one consists of at least 25%. We can just say that PANOPTESEC is able to identify and detect some of them, as in https://panoptesec.isp.uni-luebeck.de/issues/5014	NONE

Performance tests have been mainly conducted with data from the Emulation Environment, but Production Data tests have been performed (as it is detailed within Section 9). Since the Production Environment is so close to the Emulation Environment, it also uses the same data sources (GFI Languard and OpenVas are the security software Acea Areti uses for its network). It was in fact easy to run the proactive chain with data extracted from the Production Environment.

Performance of the ReachabilityMatrixCorrelator based on ontologies is sufficient in order to verify the Requirements (i.e., the complete computation time are still far under the 59 minutes identified by PRF001 and PRF007). However, during the course of the project it was also considered that better performance could improve the industrial positioning of the project. This led to the development of a ReachabilityMatrixCorrelator that is not based on ontologies and which increases performances from 9-10 minutes to 2-5 seconds on the latest version. While use of ontologies allows the system administrator to be very flexible on the description of the elements of the Monitored System, of the definition of the behaviour of the components with respect to firewall rules and routing tables, etc., this flexibility comes at the cost of slow computation times. The performance situation is improved through use of a non-ontology based component. However, this should not diminish the value of the ontology based scientific research that has been conducted in development of the intended ReachabilityMatrixCorrelator.

Since the new version of the ReachabilityMatrixCorrelator is currently used for the Operational Workshops, its performances have been tested (several Test Executions are referred to the new ReachabilityMatrixCorrelator).

The actual performances results for the proactive chain are more than sufficient from a demonstration perspective (and they completely verify the Performance Requirements): the complete chain is computed (Emulation Environment with around 160 devices, 570 vulnerabilities and 3 hypothetic entrypoints), with the new ReachabilityMatrixCorrelator, within an average of 4 minutes and 50 seconds with a 16 Gb RAM VM plus another VM with 7 Gb of ram for the SRD component (with respect to the tests reported on other Verification Reports, the number of vulnerabilities of the actual tests is higher. Some very exploitable nodes have been added in order to better show the System during the Operational Workshops). If we consider the Production Environment with around 180 devices, performances are similar (average 3 minutes, 50 seconds). Tests with thousands of devices have been conducted (using a combination of real devices and “clones” of existing devices within the NetworkInventory) and it is stated that the PANOPTESEC System proactive chain can theoretically scale up to 10k nodes keeping computation times under 59 minutes. More details can be found on Section 8.

From a reactive perspective, it has been recorded that from the reception of a Syslog with an alert within LLC to the instantiation of an Instantiated Attack Path (pointing out to the security operator that a probable attack is on-going over a particular path) by one of the correlators and the subsequent computation of the Reactive Risk by the Agg-Trq component the PANOPTESEC System took, in average, less than one minute. Other performances tests have been reported within [D422R] (resubmission) and in Section 8 of this deliverable.

4.3.4 Portability Requirements Verification

ID	Description	Importance	Test Case ID	Component(s)
PRT001	PANOPTESEC Components SHOULD be developed in a language that is portable between most current operating systems (e.g., JAVA).	2	TC.PRT001.1	Integration_Framework
PRT002	JAVA compliant interfaces MUST be provided by PANOPTESEC Components not written in JAVA.	3	TC.PRT002.1	Integration_Framework
PRT003	PANOPTESEC Components SHOULD NOT require Operating System specific libraries.	2	TC.PRT003.1	Integration_Framework
PRT004	PANOPTESEC Components design MUST follow a component-oriented model in order to enhance reuse and separation of concerns.	3	TC.PRT004.1	Integration_Framework
PRT005	PANOPTESEC Component designs MUST offer a clear and stable set of interfaces for use by other internal or external components.	3	TC.PRT005.1	PANOPTESEC System Design
PRT006	It SHOULD he possible to host the various PANOPTESEC Components in virtual machines.	2	TC.PRT006.1	Integration_Framework

4.3.5 Reliability Requirements Verification

ID	Description	Importance	Test Case ID	Component(s)
RLB001	Unit test cases MUST be created for each PANOPTESEC component.	3	TC.RLB001.1	All components / Integration_Framework
RLB002	Unit test cases MUST be updated during the PANOPTESEC project according to results from experimentation.	3	TC.RLB002.1	All components
RLB003	Updated unit test cases MUST be performed before any integration to ensure non-regression.	3	TC.RLB003.1	All components
RLB004	The PANOPTESEC architecture SHOULD be designed to tolerate faults in any of its components.	2	TC.RLB004.1 TC.RLB004.2 TC.RLB004.3 TC.RLB004.4 TC.RLB004.5	PANOPTESEC System / Integration_Framework
RLB005	In operational contexts, redundancy SHOULD be provided for databases in the PANOPTESEC system.	2	TC.RLB005.1	Repository
RLB006	In operational contexts, databases in the PANOPTESEC system MUST be regularly backed-up.	3	TC.RLB006.1	Repository
RLB007	The PANOPTESEC system MUST not impact the operational environment (i.e., the monitored or protected systems) when experiencing a failure.	3	TC.RLB007.1	All components
RLB008	Recovery time of any PANOPTESEC component	2	TC.RLB008.1	All components /

ID	Description	Importance	Test Case ID	Component(s)
	SHOULD be in the order of minutes.			Integration_Framework
RLB009	Activities of the PANOPTESEC system on hosts or on the network MUST not cause events that would be detected of suspicious (for instance causing an IDS to raise an alert).	3	TC.RLB009.1	PANOPTESEC Simulation Environment
RLB010	To avoid PANOPTESEC processing issues (e.g., race conditions or processing locks), the proactive and reactive response chains SHOULD use the same data representing the state of the Monitored System(s) as an input during the whole instance of a given computation.	2	TC.RLB010.1 TC.RLB010.2	All components / Integration_Framework
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.	3	TC.RLB011.1 TC.RLB011.2	All components / Integration_Framework
RLB012	Control loops that may result from interaction between components of the PANOPTESEC System MUST be identified.	3	TC.RLB012.1	PANOPTESEC System Design
RLB013	Control loops that may result from interaction between components of the PANOPTESEC System and the monitored system(s) MUST be identified.	3	TC.RLB013.1	PANOPTESEC System Design
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.	3	TC.RLB014.1	PANOPTESEC System Design

Summary and rationale of non-verified requirements:

Requirement			Motivation	Expected Impact
ID	Description	I		
RLB004	The PANOPTESEC architecture SHOULD be designed to tolerate faults in any of its components.	2	The development of the PANOPTESEC System considered this requirement as not completely achievable (being a SHOULD Requirement, it is acceptable). Complete fault tolerance features require an engineering effort not possible for a research prototype. Work Package 7 realized, however, a subset of the needed features, focusing on fail-over mechanisms. At the actual status of development, all integrated components benefit of the Apache Karaf failover features (at the group of components level), while a more grained proprietary technology has been developed in order to manage the failover of a	This Requirement will not be fully fulfilled, which is considered acceptable by the consortium, the PANOPTESEC System being a TRL6 research prototype

Requirement			Motivation	Expected Impact
ID	Description	I		
			single integrated (and compliant) component. At the current stage, only a subset of the components implements this mechanism.	
RLB010	To avoid PANOPTESEC processing issues (e.g., race conditions or processing locks), the proactive and reactive response chains SHOULD use the same data representing the state of the Monitored System(s) as an input during the whole instance of a given computation.	2	The degree of verification of this requirement is high. The proactive chain completely verifies the Requirement. For the Reactive chain it has been decided to not fulfil completely the requirement due to performance reasons, accepting the possibility of inconsistency between the LowLevelCorrelator Monitored System awareness and the High Level Online Correlator Monitored System awareness, which should be well handled by the High Level Online Correlators.	The proactive chain completely fulfils the requirement. At the cost of inconsistencies, the reactive one greatly increase performance and the awareness on the MonitoredSystem by the LowLevelCorrelator (being the component receiving the raw alerts, it needs to be as aware as possible of the assets of the Monitored System). The Reactive Chain, however, does not risk processing locks

4.3.6 Security Requirements Verification

ID	Description	Importance	Test Case ID	Component(s)
SEC001	The correlation results from the PANOPTESEC system SHOULD be stored in encrypted form.	2	TC.SEC001.1	Repository
SEC002	Devices that implement the PANOPTESEC system components SHOULD limit services exposure.	2	TC. SEC002.1	Integration_Framework
SEC003	Communications between the PANOPTESEC System components SHOULD be authenticated.	2	TC. SEC003.1	Integration_Framework
SEC004	Communications between the PANOPTESEC system components SHOULD be encrypted.	2	TC. SEC004.1	Integration_Framework
SEC005	User access to the PANOPTESEC system SHOULD require authentication based on individual user identification and password.	2	TC. SEC005.1	Authentication Server
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).	2	TC. SEC006.1	PANOPTESEC System / PANOPTESEC System Design

Summary and rationale of non-verified requirements:

Requirement			Motivation	Expected Impact
ID	Description	I		
SEC001	The correlation results from the PANOPTESEC system SHOULD be stored in encrypted form.	2	It has been tested that the chosen database technology (PostgreSQL) is able to allow encryption in various forms, including single columns encryption, which has been tested positively. A full implementation of the encrypted database, however, has not been installed. Being a SHOULD Requirement, this has been considered acceptable	Tests carried out and the known state of the art will allow to satisfy this requirement in fully operational environments.

4.3.7 Usability Requirements Verification

ID	Description	Importance	Test Case ID	Component(s)
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.	3	TC. USG001.1	Visualization System
USG002	Usability of the PANOPTESEC system MUST be verified and improved through regular validation by final users.	3	TC. USG002.1	Visualization System
USG003	The PANOPTESEC user interface and visualization component SHOULD be reactive to allow efficient user interactions.	2	TC.USG003.1	Visualization System

4.4 Functional Requirements

[D2.2.1] Functional Requirements have been carefully tested between Month 33 and Month 34, while some Test Executions have been repeated within Month 35. For each Requirement, from 1 to 10 Test Cases have been developed: each Requirement has been tested with respect to its traceability link with other Requirements (for example, the verification of the *derived* and *refine* Requirements have been tested for each Requirement in consideration. By acting this way, it is possible to make an already strong assessment of the verification of the Requirement itself). Of course, integration and component tests have also been made in order to complete the assessment. Several Test Executions related to the ICA requirements have been repeated in order to test the new version of the Reachability Matrix Correlator. Even if, with respect to the [D7.4.1] version of the software only few new Visualization requirements have been considered as verified, the Visualization System of the PANOPTESEC System has been greatly improved from a graphical perspective, with the aim of improving usability towards the Operational Workshops. In addition, bugfixes activities have been widely performed over all the views of the visual analytic environment.

4.4.1 Data Source Collection Requirements Verification

ID	Description	Importance	Test Case ID	Component(s)
DSC001	The PANOPTESEC system MUST provide a data collection system	3	TC.DSC001.1 TC.DSC002.1	Data Collection System
DSC002	The data collection system MUST provide a standard based interface for data collection from data sources forming part of the monitored system (s).	3	TC.DSC002.1	DeployedAccessControlPolicyCollector, NetworkInventoryProcessor, VulnerabilityInventoryProcessor, LowLevelCorrelator, NetworkDependencyAnalyser
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).	3	TC.DSC003.1	VulnerabilityAdvisoryCollector, StrategicResponseDeciderProxy, ReachabilityMatrixCorrelatorBundle
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.	3	TC.DSC004.1	DeployedAccessControlPolicyCollector, NetworkInventoryProcessor, VulnerabilityInventoryProcessor
DSC005	The data collection system SHOULD store all raw data received by the PANOPTESEC system from the monitored and non-monitored system (s).	2	TC.DSC005.1 TC.DSC005.2	Repository, DeployedAccessControlPolicyCollector, NetworkInventoryProcessor, VulnerabilityInventoryProcessor, LowLevelCorrelator, NetworkDependencyAnalyser
DSC006	The data collection system MUST collect system configuration information.	3	TC.DSC006.1 TC.DSC006.2 TC.DSC006.3 TC.DSC006.4	NetworkInventoryProcessor
DSC007	The system configuration information MUST contain information about the information communications technology (ICT) devices of the monitored system (s).	3	TC.DSC007.1 TC.DSC007.2	NetworkInventoryProcessor
DSC008	The ICT system configuration information MUST contain information about the operating systems running on the ICT devices.	3	TC.DSC008.1 TC.DSC008.2	NetworkInventoryProcessor
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).	1	TC.DSC009.1 TC.DSC009.2	NetworkInventoryProcessor
DSC010	The ICT system configuration information MAY contain information about the root certificates installed on the ICT	1	TC.DSC010.1	NA

	devices (SSL/TLS);			
DSC011	The ICT system configuration information MUST contain information about the firmware installed on the ICT devices.	3	TC.DSC011.1 TC.DSC011.2	NetworkInventoryProcessor
DSC012	The ICT system configuration information MUST contain information about the software applications running on the ICT devices.	3	TC.DSC012.1 TC.DSC012.2	NetworkInventoryProcessor
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).	3	TC.DSC013.1 TC.DSC013.2	NetworkInventoryProcessor
DSC014	The ICT system configuration information MUST contain information about the layer 3 network topology.	3	TC.DSC014.1 TC.DSC014.2	NetworkInventoryProcessor
DSC015	The ICT system configuration MUST contain information about both human and machine users and their permissions.	3	TC.DSC015.1 TC.DSC015.2 TC.DSC015.3	NetworkInventoryProcessor
DSC016	The ICT system configuration information about users and their permissions MAY include permissions for file system access.	1	TC.DSC016.1 TC.DSC016.2	NetworkInventoryProcessor
DSC017	The data collection system MUST collect security policy information.	3	TC.DSC017.1 TC.DSC017.2 TC.DSC017.3	NetworkInventoryProcessor, DeployedAccessControlPolicyCollector
DSC018	The system configuration information MUST contain information about the Supervisory Control and Data Acquisition (SCADA) devices on the monitored system (s).	3	TC.DSC018.1 TC.DSC018.2	NetworkInventoryProcessor
DSC019	The SCADA system configuration information MUST contain information about the software applications running on the SCADA devices.	3	TC.DSC019.1 TC.DSC019.2	NetworkInventoryProcessor
DSC020	The SCADA system configuration information MUST contain information about the multiple instances of firmware running on the SCADA devices.	3	TC.DSC020.1 TC.DSC020.2	NetworkInventoryProcessor
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.	3	TC.DSC021.1 TC.DSC021.2	NetworkInventoryProcessor

DSC022	Security policy management MUST support complex organizational structures including multiple partners, affiliates or subsidiaries each having different security authorities.	3	TC.DSC022.1	StrategicResponseDecider
DSC023	The data collection system MUST collect information describing the operational (or business) missions supported by the monitored system (s).	3	TC.DSC023.1 TC.DSC023.2 TC.DSC023.3	VisualizationProxyBundle, BusinessMIssionCollector, MissionImpactModule
DSC024	The operation (or business) mission information MAY be automatically collected from system configuration information.	1	TC.DSC024.1	BusinessMissionCollector
DSC025	It MUST be possible to collect operation (or business) mission information from operator input.	3	TC.DSC025.1 TC.DSC025.2	Visualization System, VisualizationProxyBundle
DSC026	The data collection system MUST collect information forming a pre-configured list of authorized operator mitigation actions.	3	TC.DSC026.1 TC.DSC026.2	VIsualizationProxyBundle
DSC027	It MUST be possible for the list of authorized operator mitigation actions to be collected from manual input	3	TC.DSC027.1	VIsualizationProxyBundle
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, Bugtrac, etc.) including at least one from Europe and one from the USA.	3	TC.DSC028.1 TC.DSC028.2	VulnerabilityAdvisoryCollector
DSC029	The data collection system MUST collect network and system events (e.g., cyber security alerts from intrusion detection systems).	3	TC.DSC029.1 TC.DSC029.2	LowLevelCorrelator
DSC030	The data collection system MUST collect information about the deployed sensors and IDSes and their configuration.	3	TC.DSC030.1 TC.DSC030.2	NetworkInventoryProcessor
DSC031	The data collection system MUST collect information about devices physical location.	3	TC.DSC031.1 TC.DSC031.2	NetworkInventoryProcessor
DSC032	The ICT system configuration information SHOULD contain information about the layer 2 network topology.	2	TC.DSC032.1 TC.DSC032.2	NetworkInventoryProcessor
DSC033	The ICT system configuration information MAY contain information about the layer 1 network topology.	1	TC.DSC033.1	NA

Summary and rationale of non-verified requirements:

Requirement			Motivation	Expected Impact
ID	Description	I		
DSC010	The ICT system configuration information MAY contain information about the root certificates installed on the ICT devices (SSL/TLS);¶	1	This Requirement is not verified, because the functionality has not been developed. The rest of the PANOPTESEC System does not need information about root certificates. Since the Requirement is a MAY, there is no impact over the rest of the system.	NONE
DSC024	The operation (or business) mission information MAY be automatically collected from system configuration information.	1	This Requirement is partially verified. The consortium developed a component, BusinessMissionCollector, able to automatically collect and translate BPMN files describing business processes into a MissionGraph, but this component has not been integrated within the PANOPTESEC System, because the User Agency (Acea) does not implement a unified business processes management system. Since the Requirement has importance 1, there is no impact over the rest of the system.	NONE
DSC033	The ICT system configuration information MAY contain information about the layer 1 network topology.	1	This Test Case cannot be verified. The PANOPTESEC System is not able to collect any layer 1 information, except the geolocalization. The requirement has not been then fulfilled, but since the Requirement has importance 1, there is no impact over the rest of the system.	NONE

As a conclusion, all importance 2 and 3 requirements are verified. Non-verified requirements have been justified, and all of them have Importance 1.

4.4.2 Information Correlation and Abstraction Requirements Verification

ID	Description	Importance	Test Case ID	Component(s)
ICA001	The PANOPTESEC system MUST contain an information correlation engine.	3	TC.ICA001.1 TC.ICA001.2	NetworkDependencyAnalyser, NetworkInventoryProcessor, VulnerabilityInventoryProcessor, LowLevelCorrelator, ReachabilityMatrixCorrelator
ICA002	The information correlation engine SHOULD translate multisource information received by the data collection system into a semantic (logic-based) common information representation.	2	TC.ICA002.1 TC.ICA002.2	NetworkDependencyAnalyser, NetworkInventoryProcessor, VulnerabilityInventoryProcessor, LowLevelCorrelator, ReachabilityMatrixCorrelator
ICA003	The information correlation engine MUST identify common information elements across the multi-source information received by the data collection system.	3	TC.ICA003.1 TC.ICA003.2	NetworkDependencyAnalyser, NetworkInventoryProcessor, VulnerabilityInventoryProcessor, LowLevelCorrelator, ReachabilityMatrixCorrelator

ICA004	The information correlation engine MUST resolve conflicts between information elements across the multi-source information received by the data collection system.	3	TC.ICA004.1 TC.ICA004.2	NetworkDependencyAnalyser, NetworkInventoryProcessor, VulnerabilityInventoryProcessor, LowLevelCorrelator, ReachabilityMatrixCorrelator
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.	3	TC.ICA005.1 TC.ICA005.2	NetworkDependencyAnalyser, NetworkInventoryProcessor, VulnerabilityInventoryProcessor, LowLevelCorrelator, ReachabilityMatrixCorrelator
ICA006	The information correlation engine MUST store all information correlation results in the PANOPTESEC system.	3	TC.ICA006.1 TC.ICA006.2	NetworkDependencyAnalyser, NetworkInventoryProcessor, VulnerabilityInventoryProcessor, LowLevelCorrelator, ReachabilityMatrixCorrelator
ICA010	The PANOPTESEC system MUST include a mission impact model.	3	TC.ICA010.1 TC.ICA010.2	MissionImpactModule
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).	3	TC.ICA011.1 TC.ICA011.2 TC.ICA011.3	MissionImpactModule
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).	3	TC.ICA012.1 TC.ICA012.2 TC.ICA012.3	MissionImpactModule
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).	3	TC.ICA013.1 TC.ICA013.2 TC.ICA013.3	MissionImpactModule
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).	3	TC.ICA014.1 TC.ICA014.2 TC.ICA014.3	MissionImpactModule
ICA015	The mission impact model MUST be able to identify mission critical systems supporting the mission (or business operations).	3	TC.ICA015.1 TC.ICA015.2 TC.ICA015.3	MissionImpactModule
ICA016	The identified mission critical systems MUST encompass mission critical software applications running on ICT devices supporting the mission (or business operations).	3	TC.ICA016.1 TC.ICA016.2 TC.ICA016.3	MissionImpactModule
ICA017	The identified mission critical systems MUST encompass mission critical software applications running on SCADA devices supporting the mission (or business operations).	3	TC.ICA017.1 TC.ICA017.2 TC.ICA017.3	MissionImpactModule
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).	3	TC.ICA018.1 TC.ICA018.2 TC.ICA018.3	MissionImpactModule
ICA019	The mission impact model MUST describe the mission impact due to cyber security compromise of identified mission critical systems.	3	TC.ICA019.1 TC.ICA019.2	MissionImpactModule

ICA020	The mission impact model MUST describe the mission impact due to mitigation actions contained in the preconfigured list of approved operator mitigation actions.	3	TC.ICA020.1 TC.ICA020.2	MissionImpactModule

As a conclusion, all requirements are verified.

4.4.3 Proactive Response System Requirements Verification

ID	Description	Importance	Test Case ID	Component(s)
PRS001	The PANOPTESEC system MUST provide a proactive response system.	3	TC.PRS001.1 TC.PRS001.2	Dynamic Risk Management Response System
PRS002	The proactive response system MUST evaluate the potential cyber security attack paths present in the system.	3	TC.PRS002.1 TC.PRS002.2 TC.PRS002.3	AggTrq
PRS003	The proactive response system MUST evaluate the potential cyber security attack paths from hypothetical attack sources to identified mission critical systems.	3	TC.PRS003.1 TC.PRS003.2	AggTrq
PRS004	The evaluation of potential cyber security attack paths by the proactive response system MUST take into account system configuration information.	3	TC.PRS004.1 TC.PRS004.2	AggTrq
PRS005	The evaluation of potential cyber security attack paths by the proactive response system MUST take into account security policy information.	3	TC.PRS005.1 TC.PRS005.2	AggTrq
PRS006	The evaluation of potential cyber security attack paths by the proactive response system MUST take into account current vulnerability advisory information.	3	TC.PRS006.1 TC.PRS006.2	AggTrq
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.	3	TC.PRS007.1 TC.PRS007.2 TC.PRS007.3	AggTrq
PRS008	The evaluation of steady state level of risk by the proactive response system MUST take into account current mission impact information.	3	TC.PRS008.1 TC.PRS008.2	AggTrq
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 detection systems).	3	TC.PRS009.1 TC.PRS009.2	AggTrq
PRS010	The proactive response system MUST propose mitigation actions to maximally reduce the evaluated steady state level of risk to identified mission critical systems.	3	TC.PRS010.1 TC.PRS010.2 TC.PRS010.3	StrategicResponseDecider
PRS011	The mitigation actions proposed by the proactive response system MUST minimize the mission impact to identified mission critical systems.	3	TC.PRS011.1 TC.PRS011.2	StrategicResponseDecider, MissionImpactModule
PRS012	The mitigation actions proposed by the proactive response system MUST be derived from a pre-configured list of approved operator mitigation actions.	3	TC.PRS012.1 TC.PRS012.2	StrategicResponseDecider

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.	1	TC.PRS013.1	Dynamic Risk Management Response System
PRS014	The proactive response system MUST enable the operator to select proposed mitigation action for actuation.	3	TC.PRS014.1 TC.PRS014.2 TC.PRS014.3	StrategicResponseDecider, Visualization System
PRS015	The proactive response system MUST enable the operator to activate any selected mitigation action for actuation.	3	TC.PRS015.1 TC.PRS015.2 TC.PRS015.3	StrategicResponseDecider, Visualization System
PRS016	The proactive response system MUST actuate (implement) mitigation actions activated by the operator for actuation.	3	TC.PRS016.1 TC.PRS022.1 TC.PRS022.2 TC.PRS022.3 TC.PRS022.4 TC.PRS022.5 TC.PRS022.6 TC.PRS022.7 TC.PRS022.8 TC.PRS022.9 TC.PRS022.10 TC.PRS022.11 TC.PRS022.12	StrategicResponseDecider, PolicyDeployer
PRS017	The actuation (implementation) of mitigation actions MUST be policy driven, based on contextual policies and suggest the activation of the optimal mitigation actions.	3	TC.PRS017.1 TC.PRS017.2	StrategicResponseDecider
PRS022	The proactive response system MUST deploy the selected mitigation actions in the monitored system.	3	TC.PRS022.1 TC.PRS022.2 TC.PRS022.3 TC.PRS022.4 TC.PRS022.5 TC.PRS022.6 TC.PRS022.7 TC.PRS022.8 TC.PRS022.9 TC.PRS022.10 TC.PRS022.11 TC.PRS022.12	StrategicResponseDecider, PolicyDeployer

Summary and rationale of non-verified requirements:

Requirement			Motivation	Expected Impact
ID	Description	I		
PRS013	The proactive response system MAY enable hypothetical evaluation of the steady state level of risk to identified mission	1	This feature has been partially implemented. It is now possible, due to the new performances reached by the system and a slight update on the graphical user interface, to easily change the hypothetical considered entry points and	NONE

Requirement			Motivation	Expected Impact
ID	Description	I		
	critical systems through manipulation of system configuration information, vulnerability advisory information, network topology information, mission impact information and approved operator mitigation actions.		recompute the proactive analysis, giving the Security Operator more flexibility on the analysis of the Monitored System.	

As a conclusion, all importance 2 and 3 requirements are verified, while one Importance 1 Requirement has been partially verified.

4.4.4 Reactive Response System Requirements Verification

ID	Description	Importance	Test Case ID	Component(s)
RRS001	The PANOPTESEC system MUST provide a reactive response system.	3	TC.RRS001.1 TC.RRS001.2	Dynamic Risk Management Response System
RRS002	The reactive response system MUST evaluate the dynamic risk level to identified mission critical systems.	3	TC.RRS002.1 TC.RRS002.2 TC.RRS002.3	AggTrq
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).	3	TC.RRS003.1 TC.RRS003.2	AggTrq, AutomataBasedEngine, QueryBasedEngine
RRS004	The evaluation of dynamic risk level by the reactive response system MUST take into account system configuration information.	3	TC.RRS004.1 TC.RRS004.2	AggTrq
RRS005	The evaluation of dynamic risk level by the reactive response system MUST take into account security policy information.	3	TC.RRS005.1 TC.RRS005.2	AggTrq
RRS006	The evaluation of dynamic risk level by the reactive response system MUST take into account current vulnerability advisory information.	3	TC.RRS006.1 TC.RRS006.2	AggTrq
RRS007	The reactive response system MUST evaluate the dynamic risk level based on the potential cyber security attack paths present in the system.	3	TC.RRS007.1 TC.RRS007.2	AggTrq
RRS008	The evaluation of dynamic level of risk by the reactive response system MUST take into account current mission impact information.	3	TC.RRS008.1 TC.RRS008.2	AggTrq
RRS009	The reactive response system MUST propose mitigation actions to maximally reduce the evaluated dynamic level of risk to identified mission critical systems.	3	TC.RRS009.1 TC.RRS009.2 TC.RRS009.3	TacticalResponseDecider

RRS010	The mitigation actions proposed by the reactive response system MUST minimize the mission impact to identified mission critical systems.	3	TC.RRS010.1 TC.RRS010.2	TacticalResponseDecider, MissionImpactModule
RRS011	The mitigation actions proposed by the reactive response system MUST be derived from a pre-configured list of approved operator mitigation actions.	3	TC.RRS011.1 TC.RRS011.2	TacticalResponseDecider
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.	1	TC.RRS012.1	NA
RRS013	The reactive response system MUST enable the operator to select proposed mitigation action for actuation.	3	TC.RRS013.1 TC.RRS013.2 TC.RRS013.3	TacticalResponseDecider, Visualization System
RRS014	The reactive response system MUST enable the operator to activate any selected mitigation action for actuation.	3	TC.RRS014.1 TC.RRS014.2 TC.RRS014.3	TacticalResponseDecider, Visualization System
RRS015	The reactive response system MUST actuate (implement) mitigation actions activated by the operator for actuation.	3	TC.PRS022.1 TC.PRS022.2 TC.PRS022.3 TC.PRS022.4 TC.PRS022.5 TC.PRS022.6 TC.PRS022.7 TC.PRS022.8 TC.PRS022.9 TC.PRS022.10 TC.PRS022.11 TC.PRS022.12	TacticalResponseDecider, PolicyDeployer
RRS016	The reactive response system MUST be able to model, compute and process multi-step attack scenarios based on topological and business information.	3	TC.RRS016.1 TC.RRS016.2 TC.RRS016.3	AggTrq, AutomataBasedEngine, QueryBasedEngine
RRS017	The reactive response system MUST be fed automatically with complex correlation rules generated from attacks trees issued by the risk analysis phase.	3	TC.RRS017.1 TC.RRS017.2	AggTrq, AutomataBasedEngine, QueryBasedEngine
RRS018	The reactive response system MAY suggest the activation of mitigation actions based on contextual policies.	1	TC.RRS018.1	NA
RRS023	The reactive response system SHOULD benefit from the use of anomaly detection, in order to derive new attack patterns.	2	TC.RRS023.1	NA
RSS024	The reactive response system MUST deploy the selected mitigation actions in the monitored system.	3	TC.PRS022.1 TC.PRS022.2 TC.PRS022.3 TC.PRS022.4 TC.PRS022.5 TC.PRS022.6 TC.PRS022.7 TC.PRS022.8	TacticalResponseDecider, PolicyDeployer

			TC.PRS022.9 TC.PRS022.10 TC.PRS022.11 TC.PRS022.12	
RRS025	The reactive response system MUST be able to correlate alerts with multi-step attack models.	3	TC.RRS025.1 TC.RRS025.2	AggTrq, AutomataBasedEngine, QueryBasedEngine
RRS026	The reactive response system MUST be able to automatically generate multi-step attack models and correlation rules.	3	TC.RRS026.1 TC.RRS026.2	AggTrq, AutomataBasedEngine, QueryBasedEngine
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..).	2	TC.RRS027.1 TC.RRS027.2	AggTrq, AutomataBasedEngine, QueryBasedEngine

Summary and rationale of non-verified requirements:

Requirement			Motivation	Expected Impact
ID	Description	I		
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.	1	In theory, with the new performances reached by all the PANOPTESEC System components, it would be possible to manage hypothetical evaluations of the risk status while keeping the actual situation running, but the feature has not been developed. Since the Requirement has importance 1, there is no impact over the rest of the system.	NONE
RRS018	The reactive response system MAY suggest the activation of mitigation actions based on contextual policies.	1	This Test Case cannot be verified, since the reactive system does not need any contextual policy for the activation. Since the requirement has only low importance, it is not considered critical.	NONE
RRS023	The reactive response system SHOULD benefit from the use of anomaly detection, in order to derive new attack patterns.	2	This requirement is mainly related to the envisioned optional component Potential Attack Identifier from [D3.1.2]. Since this component has not been developed, the TC fails. Due to the fact that Importance of the requirement is 2, it is not considered as critical	NONE

As a conclusion, all importance 3 requirements are verified. Non-verified requirements have been justified.

4.4.5 Visualization Requirements Verification

ID	Description	Importance	Test Case ID	Component(s)
VIZ001	The PANOPTESEC MUST provide a visualization system that displays cyber defense situational awareness in real-time.	3	TC.VIZ001.1 TC.VIZ001.2	Visualization 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.	3	TC.VIZ002.1 TC.VIZ002.2 TC.VIZ002.3	Visualization System
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.	3	TC.VIZ003.1 TC.VIZ003.2	Visualization System
VIZ004	The displayed cyber defense situational awareness MUST represent the dynamic risk level to identified mission critical systems derived by the reactive response system.	3	TC.VIZ004.1 TC.VIZ004.2 TC.VIZ004.3	Visualization System
VIZ005	The displayed cyber defense situational awareness MUST represent the anticipated mission impact due to the dynamic level risk to identified mission critical systems.	3	TC.VIZ005.1 TC.VIZ005.2	Visualization System
VIZ006	The visualization system MUST enable the operator to display detailed information about identified mission critical systems information.	3	TC.VIZ006.1 TC.VIZ006.2	Visualization System
VIZ007	The monitoring system MUST enable the operator to display detailed information about system configuration.	3	TC.VIZ007.1 TC.VIZ007.2	Visualization System
VIZ008	The visualization system MUST enable the operator to display detailed information about Layer 3 network topology information.	3	TC.VIZ008.1 TC.VIZ008.2	Visualization System
VIZ009	The visualization system MUST enable the operator to display detailed information about vulnerability advisory information from all sources used in the PANOPTESEC system.	3	TC.VIZ009.1 TC.VIZ009.2	Visualization System
VIZ010	The visualization system MUST enable the operator to display detailed information about cyber security attack paths information.	3	TC.VIZ010.1 TC.VIZ010.2	Visualization System
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.	3	TC.VIZ011.1 TC.VIZ011.2	Visualization System
VIZ012	The visualization system MUST display the mitigation actions proposed by the proactive response system.	3	TC.VIZ012.1 TC.VIZ012.2 TC.VIZ012.3	Visualization System
VIZ013	The visualization system MUST enable operator selection of mitigation actions proposed by the proactive response system.	3	TC.VIZ013.1 TC.VIZ013.2 TC.VIZ013.3	Visualization System
VIZ014	The visualization system MUST display the mitigation actions proposed by the reactive response system.	3	TC.VIZ014.1 TC.VIZ014.2 TC.VIZ014.3	Visualization System

VIZ015	The visualization system MUST enable operator selection of mitigation actions proposed by the reactive response system.	3	TC.VIZ015.1 TC.VIZ015.2 TC.VIZ015.3	Visualization System
VIZ016	The visualization system MUST enable operator activation of operator selected mitigation actions.	3	TC.VIZ016.1 TC.VIZ016.2	Visualization System
VIZ017	The visualization system MAY enable operator input of mission impact information.	1	TC.VIZ017.1 TC.VIZ017.2	Visualization System
VIZ018	The visualization system MUST enable the operator to designate systems as identified mission critical systems.	3	TC.VIZ018.1 TC.VIZ018.2 TC.VIZ018.3	Visualization System
VIZ019	The visualization system MUST enable the operator to enter a mission impact description for security compromise to identified mission critical systems.	3	TC.VIZ019.1 TC.VIZ019.2	Visualization System
VIZ020	The visualization system MAY enable detailed display of raw information available in the PANOPTESEC system.	1	TC.VIZ020.1	NA
VIZ021	The visualization system MUST provide information about the actual system vulnerabilities	3	TC.VIZ021.1 TC.VIZ021.2 TC.VIZ021.3	Visualization System
VIZ022	The visualization system representation of actual system vulnerabilities MUST differentiate between exploitable and non-exploitable vulnerabilities.	3	TC.VIZ022.1 TC.VIZ022.2	Visualization System
VIZ023	The PANOPTESEC visualization system SHOULD enable historical data analysis.	2	TC.VIZ021.1 TC.VIZ021.2 TC.VIZ021.3	Visualization System
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).	2	TC.VIZ022.1 TC.VIZ022.2 TC.VIZ022.3	Visualization System
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.	2	TC.VIZ025.1 TC.VIZ025.2	Visualization System
VIZ026	The visualization system MUST allow an operator to ask for stopping a reactive mitigation action to an ongoing attack.	3	TC.VIZ026.1 TC.VIZ026.2	Visualization System
VIZ027	The visualization system SHOULD provide the operator with representations to estimate the consequences of an ongoing attack	2	TC.VIZ027.1 TC.VIZ027.2	Visualization System
VIZ028	The visualization system SHOULD provide the operator with mechanisms to easily share any information about the situation.	2	TC.VIZ028.1 TC.VIZ028.2	Visualization System
VIZ029	The visualization system SHOULD enable the operator to display detailed information about Layer 2 network topology information.	2	TC.VIZ029.1	NA
VIZ030	The visualization system MAY enable the operator to display detailed information about Layer 1 network topology information.	1	TC.VIZ030.1	NA

Summary and rationale of non-verified requirements:

Requirement			Motivation	Expected Impact
ID	Description	I		
VIZ020	The visualization system MAY enable detailed display of raw information available in the PANOPTESEC system.	1	This Test Case cannot be verified: the detailed display of raw info is not available at the current state. Since the associated requirement is not mandatory (nor critical) the development of this functionality is not considered a major need for PANOPTESEC system in order to reach its goals.	NONE
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.	2	While it is possible for the operator to shift the analysis focal point forward and back in time, no automatic comparison between snapshots is given. Since the requirements is not mandatory and it is partially fulfilled, the consortium decided to not develop it further	NONE
VIZ029	The visualization system SHOULD enable the operator to display detailed information about Layer 2 network topology information.	2	This Test Case cannot be verified: the display of detailed information about Layer 2 network topology information is not available. Information regarding MAC addresses, however, are available. Since the associated requirement is not mandatory (nor critical) the development of this functionality is not considered a major need for PANOPTESEC system in order to reach its goals.	NONE
VIZ030	The visualization system MAY enable the operator to display detailed information about Layer 1 network topology information.	1	This Test Case cannot be verified: the display of detailed information about Layer 1 network topology information is not available at the current state. Since the associated requirement has just Importance 1, the development of this functionality is not considered a major need for PANOPTESEC system in order to reach its goals.	NONE

As a conclusion, all importance 3 requirements are verified and almost all importance 2 requirements have been verified.

4.5 Conclusions

As can be seen in the previous Sections, all Importance 3 System Level Requirements have been verified by the PANOPTESEC System. Most of the Importance 2 have been verified and even many Importance 1 have been verified. All non-verified requirements have been justified and identified as non-interesting for the purpose of the PANOPTESEC System and will not be developed. This behavior is fully compatible with any software project and is even more acceptable within a research project.

From an overall perspective, the PANOPTESEC System is considered verified against its System Level Requirements from [D2.2.1].

5 PANOPTESEC SYSTEM COMPONENTS INTEGRATION TESTS

The [D4.3.1], [D5.4.1] and [D6.3.1] software deliverables are composed of a set of components ready for integration with the rest of the PANOPTESEC System.

In order to assess that the Data Collection and Correlation Integration Prototype, the Response System for Dynamic Risk Management Integration Prototype and the Visualization System Integration Prototype are correctly integrated after the final integration phase executed during month 33 and 34, it is necessary to verify that all interactions between WP4, WP5 and WP6 components (as depicted in the PANOPTESEC System Design) are actually implemented. Since this activity involves the Integration Framework, these Integration Tests between WP4, WP5 and WP6 components have been conducted by the Work Package 7 and they are encompassed on the set of Integration Tests conducted by WP7 (which regards the complete system). Most of the Test Cases for the Verification of [D2.2.1] requirements summarized within Section 4, in fact, involve the complete or partial integration of the various components of the PANOPTESEC System.

In order to fill the gap between the High-Level Design and the code implementation, a Low-Level Design, focused on integration, messaging and interfaces, has been developed. It directly derives from the High-Level Design (the two Designs, linked by traceability links, are available within the Papyrus Project part of the [D7.4.1]).

All Design/Integration Test Cases and the corresponding Test Executions can be found within the Design Project in the Redmine website (https://panoptesec.isp.uni-luebeck.de/projects/design).

Not all Test Executions have been repeated, if the involved components did not change in terms of interfaces and behavior, but both the proactive and the reactive chain have been carefully verified again against the related Sequence Diagrams.

All repeated Test Executions have been performed over the 23 September 2016 version of the prototypes and the Design.

5.1.1 Caption

Colour	TC Exists?	TE Exists?	Outcome	Redmine Documentation Status
	N	N	N	
	Y	N	N	In Progress
	Y	Y	N (all TEs fail)	Rejected
	Y	Y	Partial (not 100% TEs succeeds)	In Progress
	Y	Y	Y	Resolved

Table 6 – Color Coding Used for the final assessment of Design Verification

Some of tests are conducted by code inspection, with the aim to show that the components correctly implement the defined interfaces. For the interactions between components of

the PANOPTESEC System, however, complex integration tests are conducted in order to show the coverage of the so far integrated system with the design orchestration in the Sequence Diagrams depicted in [D7.4.1].

5.1.2 Integration Tests

ID	Test Case ID	Component(s)
IF	TC.IF.1	Integration Framework / all PANOPTESEC System components
	TC.IF.2	
	TC.IF.3	
	TC.IF.4	
	TC.IF.5	

The PANOPTESEC System is still completely integrated as for the 23 September 2016 Version of the system. Under the Performance Non-Functional Requirement Section 4.3.3 it is possible to check that performances have been carefully tested and improved during months 33 and 34 and 35 in order to meet the specifications and to test the boundaries of the system.

These set of tests clearly show that WP4, WP5 and WP6 components are integrated between them and with the rest of the PANOPTESEC System following the specifications from the design. All interfaces depicted in the High and Low Level Designs are correctly implemented, as for all integration dependencies.

6 PANOPTESEC SYSTEM REQUIREMENTS VALIDATION

6.1 Introduction

PANOPTESEC System Validation methodology is described in Section 2.2.1. The Validation, which follows the complete Verification phase whose results are described within Section 3 and 4, started with the feedbacks from internal stakeholders (from the User Agency -the teams involved in the definition of the system-level requirements described within [D2.2.1]-, from the External Advisory Board of the project and from all project members), after detailed and holistic demonstrations of the PANOPTESEC System during the end of Month 35. These first demonstrations, in addition, constituted a source of information when the Consortium performed the Qualification Review on 11th October 2016.

6.2 Internal Stakeholders Workshops and surveys

6.2.1 Organization of the Workshops

Among the activities around [D8.2.2], the Installed Prototype has been demonstrated with a first round of Operational Workshops, with the aim of validating the prototype towards the Qualification Review (held on 11th October 2016).

The Workshops for the QR have been organised among 4 sessions:

- Multiple intra-Consortium live demo (20-21 September 2016), in order to validate the presentation itself with all partners (no surveys have been conducted for these internal demo, but the general feedback was important in order to perform the last refinements);
- 22nd of September 2016: with internal stakeholders from Acea (with surveys);
- 23rd of September 2016 with the EAB (with surveys);
- 5th of October 2016 with internal stakeholder from Acea (with surveys).

These Workshops involved a Live Demo of the PANOPTESEC System through a set of demonstration activities involving attacks scenarios, cyber security awareness status analysis and up-to-date project results in order to receive Acea Group end-users and EAB feedbacks in order to validate the prototype itself. Every considered Demonstration Activity was taken from [D8.2.1], with traceability links with the System-Level Requirements from [D2.2.1}.

Proactive scenarios addressed use cases involving collection, correlation and analysis of infrastructure and non-infrastructure (e.g., public vulnerability awareness) data. Reactive scenarios addressed detection, analysis and response to active attacks.

Each demonstration lasted from 2.5 to 5 hours, while attendees could interact and make questions and comments about the PANOPTESEC System.

During the demonstrations, after each chapter/scenario, attendees were asked to fill the feedback questionnaire section dedicated to the specific Demonstration Activity.

All attendees belonging to Acea Group were not directly involved in the PANOPTESEC Project (but some of them participated to the Requirements Elicitation phase from Month 1 to 4), except for Alessandro Iacomini who works as network administrator in the Command and Control network of Areti (former Acea Distribuzione Energia).

In Table 7 the list of attendees, their company and role:

Table 7: first Operational Workshops list of attendees

Name/Surname	Company	Role/Dpt
Enrico De Castro	Acea SpA	ICT/SOC
Francesco Branchitta	Acque SpA	IT Manager
Paolo Del Vita	Acquedotto del Fiora SpA	ICT Consultant
Daniele Nigro	Acquedotto del Fiora SpA	ICT Consultant
Claudio Caria	Areti Spa	Remote control system operator

Name/Surname	Company	Role/Dpt
Giovanni Delli Quadri	Areti Spa	Responsible of Operations
Alessandro Iacomini	Areti Spa	SCADA network administrator
Andrea de Caterini	GEAL SpA	CEO
Francesco Fossati	Ingegnerie Toscane SpA	Responsible of SCADA systems
Damasco Morelli	Ingegnerie Toscane SpA	Technical Director
Ronald Rietveld	Cyber Guard International	EAB
Wim Mees	Royal Military Academy	EAB
Nikolai Stoianov	Defense Institute, Sofia	EAB
Salvador Llopis	European Defence Agency	EAB
Lorenzo Balucca	Umbra Acque SpA	Responsible of SCADA systems
Paolo Salari	Umbra Acque SpA	IT Manager
Raffaele D'Auria	Acea ATO 5 SpA	Responsible of SCADA systems
Pietro Marta	Acea ATO 2 SpA	Responsible of SCADA systems
Roberto Celestini	Acea ATO 2 SpA	Head water control room
Lorenzo Arrighetti	Acea ATO 2 SpA	Head Dispaching supervisor
Ercole de Luca	Acea SpA	Energy Management

Among them, Mr De Castro could not attend the whole workshop and did not fulfill the questionnaire.

6.2.2 Results of the surveys

All participants expressed a general satisfaction with the demonstrated PANOPTESEC System.

Out of 25 filled questionnaires and a total of 32 questions it is possible to count 439 "very good/yes" and 335 "good".

In the following figures the results are shown.

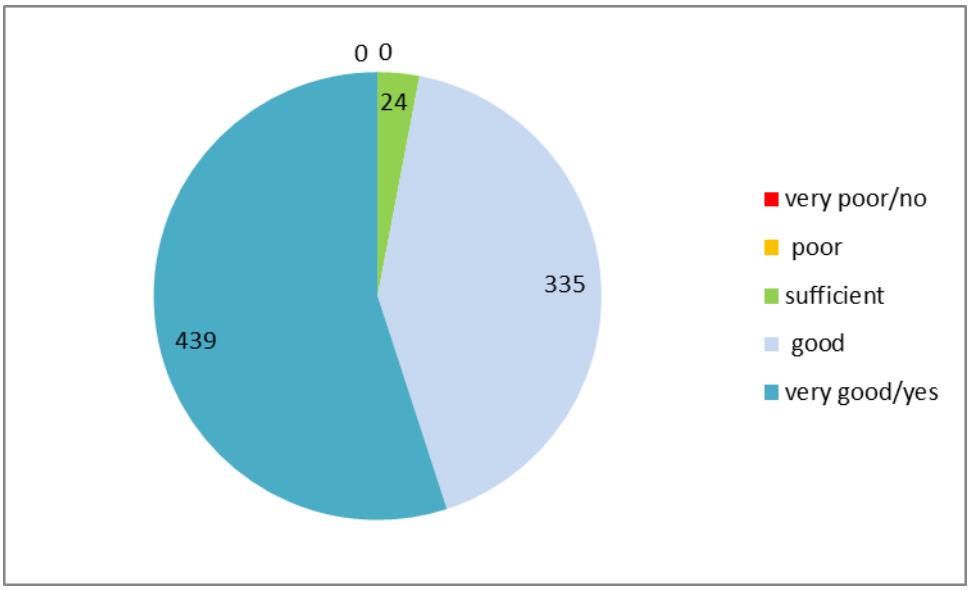


Figure 1: Overall results of the survey

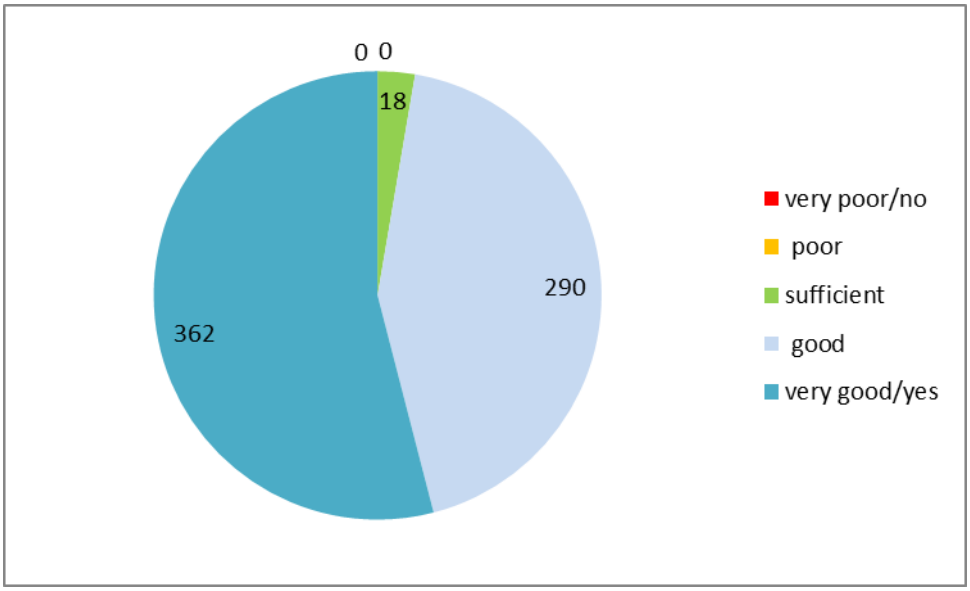


Figure 2: Results of the survey (only internal stakeholders)

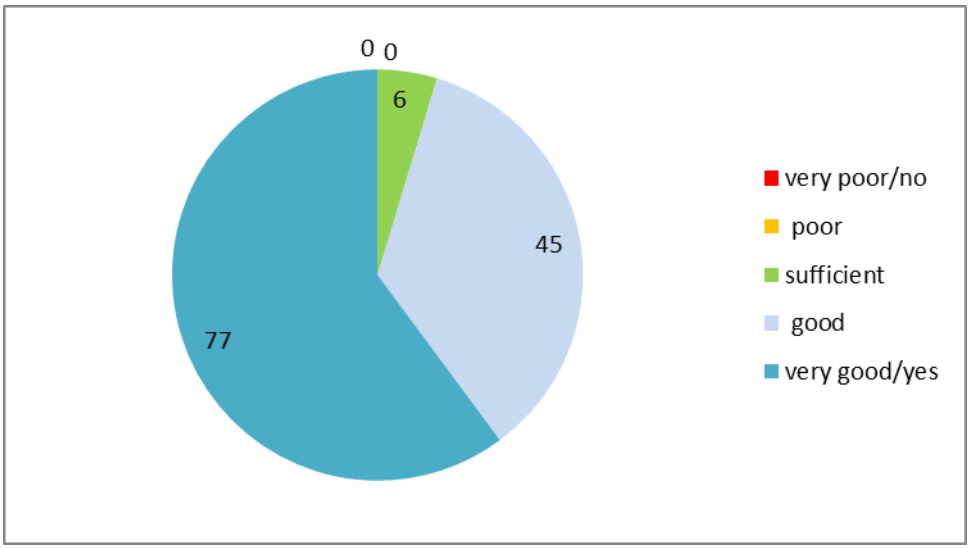


Figure 3: Results of the survey (only EAB)

The details of results are shown in the following figures divided per Demonstration Activity (from [D8.2.1]) and the additional questions.

DA01

							total					Internal stackholder					EAB				
	1:very poor/no 2: poor 3: sufficient 4: good 5:very good/yes						1	2	3	4	5	1	2	3	4	5	1	2	3	4	5
DA01	**Monitored System Overview**																				
1.1	Does the System show a correct network, topology and system inventory (comprehensive asset identification) ?	1	2	3	4	5	0	0	0	9	16	0	0	0	9	12	0	0	0	0	4
1.2	Is the network, topology and system inventory appropriate for the project's goals?	1	2	3	4	5	0	0	0	9	16	0	0	0	8	13	0	0	0	1	3
1.3	Is the network reconstruction showing useful geographical information?	1	2	3	4	5	0	0	1	8	16	0	0	1	7	13	0	0	0	1	3

DA02

							total					Internal stackholder					EAB				
	1:very poor/no 2: poor 3: sufficient 4: good 5:very good/yes						1	2	3	4	5	1	2	3	4	5	1	2	3	4	5
DA02	**Monitored System Vulnerability Surface**																				
2.1	Does the System show a correct vulnerability inventory (correlation of assets to known vulnerabilities) ?	1	2	3	4	5	0	0	1	10	14	0	0	1	8	12	0	0	0	2	2
2.2	Is the vulnerability inventory appropriate for the project's goals?	1	2	3	4	5	0	0	0	12	13	0	0	0	10	11	0	0	0	2	2

DA03

							total					Internal stackholder					EAB				
	1:very poor/no 2: poor 3: sufficient 4: good 5:very good/yes						1	2	3	4	5	1	2	3	4	5	1	2	3	4	5
DA03	**Monitored System Mission Impact assessment**																				
3.1	Does the System show a correct view of the business processes of the Company, correlated with the dependent ICT/SCADA devices?	1	2	3	4	5	0	0	3	8	14	0	0	1	8	12	0	0	2	0	2
3.2	Is the view of the business processes and their relationship with the ICT/SCADA device appropriate for the project's goals?	1	2	3	4	5	0	0	1	11	13	0	0	0	9	12	0	0	1	2	1

DA04

							total					Internal stackholder					EAB				
	1:very poor/no 2: poor 3: sufficient 4: good 5:very good/yes						1	2	3	4	5	1	2	3	4	5	1	2	3	4	5
DA04	**Risk Analysis, Proactive Risk and Attack Graph**																				
4.1	Does the System show a correct detection of the possible attack paths within the Monitored System, given a set of entrypoints?	1	2	3	4	5	0	0	1	8	16	0	0	1	8	12	0	0	0	0	4
4.2	Is the attack paths detection consistent with the network topology reconstruction?	1	2	3	4	5	0	0	1	12	12	0	0	1	10	10	0	0	0	2	2
4.3	Is the attack paths detection useful?	1	2	3	4	5	0	0	0	9	16	0	0	0	7	14	0	0	0	2	2
4.4	Does the System show a reconstruction of the quantification of the level of the Risk of the System?	1	2	3	4	5	0	0	0	13	12	0	0	0	11	10	0	0	0	2	2
4.5	Is the Risk quantification analysis appropriate for the project's goals?	1	2	3	4	5	0	0	0	12	13	0	0	0	10	11	0	0	0	2	2

DA05

							total					Internal stackholder					EAB				
	1:very poor/no 2: poor 3: sufficient 4: good 5:very good/yes						1	2	3	4	5	1	2	3	4	5	1	2	3	4	5
DA05	**Strategic Response Overview**																				
5.1	Does the System show a prioritized strategic dashboard, with related strategic response plans optimized by risk reduction, response on financial investment impact evaluation and operational impact evaluation?	1	2	3	4	5	0	0	0	10	15	0	0	0	8	13	0	0	0	2	2
5.2	Is the strategic response plan computation consistent with the topology of the Monitored System and the quantification of the actual level of the Risk?	1	2	3	4	5	0	0	0	12	13	0	0	0	11	10	0	0	0	1	3
5.3	Is the strategic dashboard useful?	1	2	3	4	5	0	0	2	6	17	0	0	2	4	15	0	0	0	2	2

DA06

							total					Internal stackholder					EAB				
	1:very poor/no 2: poor 3: sufficient 4: good 5:very good/yes						1	2	3	4	5	1	2	3	4	5	1	2	3	4	5
DA06	**Architecture Component Overview**																				
6.1	Is the software architecture of the Panoptesec coherent with the purposes of the Project?						0	0	0	8	16	0	0	0	7	13	0	0	0	1	3
6.2	Are the Panoptesec software security mechanisms (authentication, crtiptography, etc.) providing an adequate protection for sensitive data?	1	2	3	4	5	0	0	2	14	8	0	0	1	11	8	0	0	1	3	0

DA07

							total					Internal stackholder					EAB				
	1:very poor/no 2: poor 3: sufficient 4: good 5:very good/yes						1	2	3	4	5	1	2	3	4	5	1	2	3	4	5
DA07	**Incident Correlation Overvew (IAP analysis)**																				
7.1	Is the System able to correlate percieved security incidents with the computed attack paths?	1	2	3	4	5	0	0	0	10	15	0	0	0	9	12	0	0	0	1	3
7.2	Does the System visualize these correlation in order to alert the operator that a an attack is on going?	1	2	3	4	5	0	0	0	11	14	0	0	0	11	10	0	0	0	0	4
7.3	Is the System able to quantify the reactive level of the Risk, given a set of correlated incidents?	1	2	3	4	5	0	0	0	13	12	0	0	0	11	10	0	0	0	2	2

DA08

							total					Internal stackholder					EAB				
	1:very poor/no 2: poor 3: sufficient 4: good 5:very good/yes						1	2	3	4	5	1	2	3	4	5	1	2	3	4	5
DA08	**Tactical Response Plan**																				
8.1	Does the System show a prioritize reactive dashboard, with related tactical response plans optimized by risk reduction and operational impact evaluation?	1	2	3	4	5	0	0	0	10	15	0	0	0	8	13	0	0	0	2	2
8.2	Are the tactical response plans coherent with the percieved correlated incidents?	1	2	3	4	5	0	0	0	12	13	0	0	0	11	10	0	0	0	1	3
8.3	Is the tactical dashboard useful?	1	2	3	4	5	0	0	0	12	13	0	0	0	10	11	0	0	0	2	2

Q01

							total					Internal stackholder					EAB				
	1:very poor/no 2: poor 3: sufficient 4: good 5:very good/yes						1	2	3	4	5	1	2	3	4	5	1	2	3	4	5
Q01	**Do you think that the attack scenarios are realistic?**	1	2	3	4	5	0	0	1	7	17	0	0	1	5	15	0	0	0	2	2

Q02

							total					Internal stackholder					EAB				
	1:very poor/no 2: poor 3: sufficient 4: good 5:very good/yes						1	2	3	4	5	1	2	3	4	5	1	2	3	4	5
Q02	**Do you think that the Panoptesec response time from a proactive perspective is appropriate?**	1	2	3	4	5	0	0	1	10	14	0	0	0	9	12	0	0	1	1	2

Q03

							total					Internal stackholder					EAB				
	1:very poor/no 2: poor 3: sufficient 4: good 5:very good/yes						1	2	3	4	5	1	2	3	4	5	1	2	3	4	5
Q03	**Do you think that the Panoptesec response time from a reactive perspective is appropriate?**	1	2	3	4	5	0	0	1	9	15	0	0	0	9	12	0	0	1	0	3

Q04

							total					Internal stackholder					EAB				
	1:very poor/no 2: poor 3: sufficient 4: good 5:very good/yes						1	2	3	4	5	1	2	3	4	5	1	2	3	4	5
Q04	**Is the graphical user interface appropriate for the project's goals?**	1	2	3	4	5	0	0	2	12	11	0	0	2	12	7	0	0	0	0	4

Q05

							total					Internal stackholder					EAB				
	1:very poor/no 2: poor 3: sufficient 4: good 5:very good/yes						1	2	3	4	5	1	2	3	4	5	1	2	3	4	5
Q05	**Do you think that the Panoptesec or some part of the Panoptesec could be useful in your organization?**	1	2	3	4	5	0	0	0	9	16	0	0	0	8	13	0	0	0	1	3

Q06

							total					Internal stackholder					EAB				
	1:very poor/no 2: poor 3: sufficient 4: good 5:very good/yes						1	2	3	4	5	1	2	3	4	5	1	2	3	4	5
Q06	**Does the system provide useful information?**	1	2	3	4	5	0	0	0	9	16	0	0	0	8	13	0	0	0	1	3

Q07

							total					Internal stackholder					EAB				
	1:very poor/no 2: poor 3: sufficient 4: good 5:very good/yes						1	2	3	4	5	1	2	3	4	5	1	2	3	4	5
Q07	Does the system provide up to date information ?	1	2	3	4	5	0	0	0	13	12	0	0	0	11	10	0	0	0	2	2

Q08

							total					Internal stackholder					EAB				
	1:very poor/no 2: poor 3: sufficient 4: good 5:very good/yes						1	2	3	4	5	1	2	3	4	5	1	2	3	4	5
Q08	Is the information clear?	1	2	3	4	5	0	0	2	11	12	0	0	2	9	10	0	0	0	2	2

Q09

							total					Internal stackholder					EAB				
	1:very poor/no 2: poor 3: sufficient 4: good 5:very good/yes						1	2	3	4	5	1	2	3	4	5	1	2	3	4	5
Q09	Is the system easy to use ?	1	2	3	4	5	0	0	5	16	4	0	0	5	13	3	0	0	0	3	1

The result of the survey states a general full appreciation of the PANOPTESEC System on all demonstration activities.

Particularly the question DA05 -5.3 *"*Is *the strategic dashboard useful?", and Q01 "*Do you think that the attack scenarios are realistic?

had 17 "very good/yes" out of 25 answers.

The Q09 *"Is the system easy to use?"* received 4 "very good/yes" and 16 "good". It is an important positive feedback considering that the PANOPTESEC System it is not a commercial product but it is a research software project. This result has been possible thanks to the deep usability refinement performed over the Visualization System during Month 35.

6.2.3 Conclusions

It is possible to state an overall satisfaction of the internal stakeholders about the PANOPTESEC System. In terms of traceability of the survey result with the System Level Requirements (as detailed in [D8.2.1]), it is possible to state that from an overall perspective these Requirements from [D2.2.1] have been validated by the internal stakeholders. This result enforces the Verification activities summarized within Section 3 and 4 of this report.

6.3 Operational Workshops and surveys

6.3.1 Organization of the Workshops

After the first set of Workshops, the Installed Prototype has been validated with a set of Operational Workshops open to external stakeholders from the industry, covering banking sector, defence, SMEs, critical infrastructures, public organizations, telecommunication companies, IT companies.

The Workshops were organised on several sessions during the two weeks between 17 and 28 October 2016.

- 17/10/2016: a session in the morning and a session in the afternoon (both with a feedback survey);
- 18/10/2016: a session in the morning and a session in the afternoon (both with a feedback survey);
- 20/10/2016: a session in the morning (with a feedback questionnaire);
- 21/10/2016: a session in the morning and a session in the afternoon (both with a feedback survey);
- 24/10/2016: a session in the morning and a session in the afternoon (both with a feedback survey);
- 25/10/2016: a session in the morning and a session in the afternoon (both with a feedback survey);
- 26/10/2016: a session in the morning and a session in the afternoon (both with a feedback survey);
- 27/10/2016: a session in the morning (with a feedback questionnaire);
- 28/10/2016: a session in the morning and a session in the afternoon (both with a feedback survey);

Other sessions are scheduled for 18 and 25 November 2016.

These Workshops have been configured as a Live Demo of the PANOPTESEC System through a set of Demonstration Activities (with the same structure of the internal workshops detailed within Section 6.2) involving attacks scenarios, cyber security awareness status analysis and up-to-date project results in order to receive external stakeholders feedback to validate the prototype itself.

Proactive scenarios addressed use cases involving collection, correlation and analysis of infrastructure and non-infrastructure (e.g., public vulnerability awareness) data. Reactive scenarios addressed detection, analysis and response to active attacks.

Each demonstration took around 2-3.5 hours, while attendees could interact and make questions and comments about the PANOPTESEC System.

During the demonstrations, after each chapter/scenario, the attendees were asked to fill the feedback questionnaire section dedicated to the specific Demonstration Activity.

The ratio of organizing 18 different sessions with few very qualified attendees instead of one only crowed event was giving to each attendee time and room to deeply interact with the PANOPTESEC Consortium representatives.

During these sessions **92** external stakeholders and other **13** internal stakeholders (who could not participate to the Qualification Review) joined the Operational Workshops.

Detailed results of the Operational Workshops can be found in [D8.2.3]. This report provides a summary useful for software Validation purposes.

6.3.2 The External stakeholders

The external and qualified stakeholders belong to a number of sectors identified as strategic for the future development of the PANOPTESEC System: among these the attendees came from the following sectors/industries:

Sector & Company/public institution	Number of attendees
Aerospace, Defence& Security	**1**
Leonardo Company	1
Banks	**1**
San Paolo Inv	1
Consultancy	**3**
consultant	1
PWC Advisory	2
Defence	**9**
Commando C4 Difesa	1
Military Communication Institute (Poland)	2
Ministero Difesa	1
SM Difesa	1
SM Difesa (ITA MOD)	3
SME Difesa (ITA MOD)	1
Education/Research	**5**
CINECA	1
GARR	3
Università Roma La Sapienza	1

Energy	**2**
Meta Energia	2
European Space Agency	**2**
ESA	2
Government/Istitution	**4**
ENAC	1
Min Interno - CNAIPIC	3
IT	**45**
Acsi Informatica Srl	3
ADFL Consulting	2
Akito	3
Business-E S.p.A.	1
CMP Link Srl	2
DGS	2
EPS Datacom	1
Ericsson	1
ESET	2
Fire Eye	2
Gruppo DAMAN	1
IBM	2
Info solution	1
Innovery	1
Lutech SpA	3
NSR	3
R1 S.p.A.	8
rds lab	1
Security Matters	2
Servi tecno	1
SIRTI	3
Oil	**1**
ERG S.p.A.	1
Other	**1**
Canada Embassy	1
Postal/financial	**1**
Poste Italiane	1
Press	**2**
Cyber Affairs	1
Fly Orbit news	1
Telco&Mobile	**5**
H3G	1
TIM	4
Telecommunications	**1**

BT	1
Television	**1**
RAI	1
Trasport	**2**
Ferrovie dello Stato Italiane	2
Utility	**3**
ASM Terni SpA	2
HERA	1
SCADA and modelling	**3**
IDeA Srl	1
Proteo	1
Schneider-Electric	1
Totale complessivo	**92**

6.3.3 Results of the surveys for the external stakeholders

All participants expressed a general satisfaction with the demonstrated PANOPTESEC System.

Out of 91 filled questionnaires and a total of 2941 questions it is possible to count 1526 “very good/yes (5)” and 1113 “good (4)” with an overall average of 4,49.

In the following figures, detailed results of the surveys:

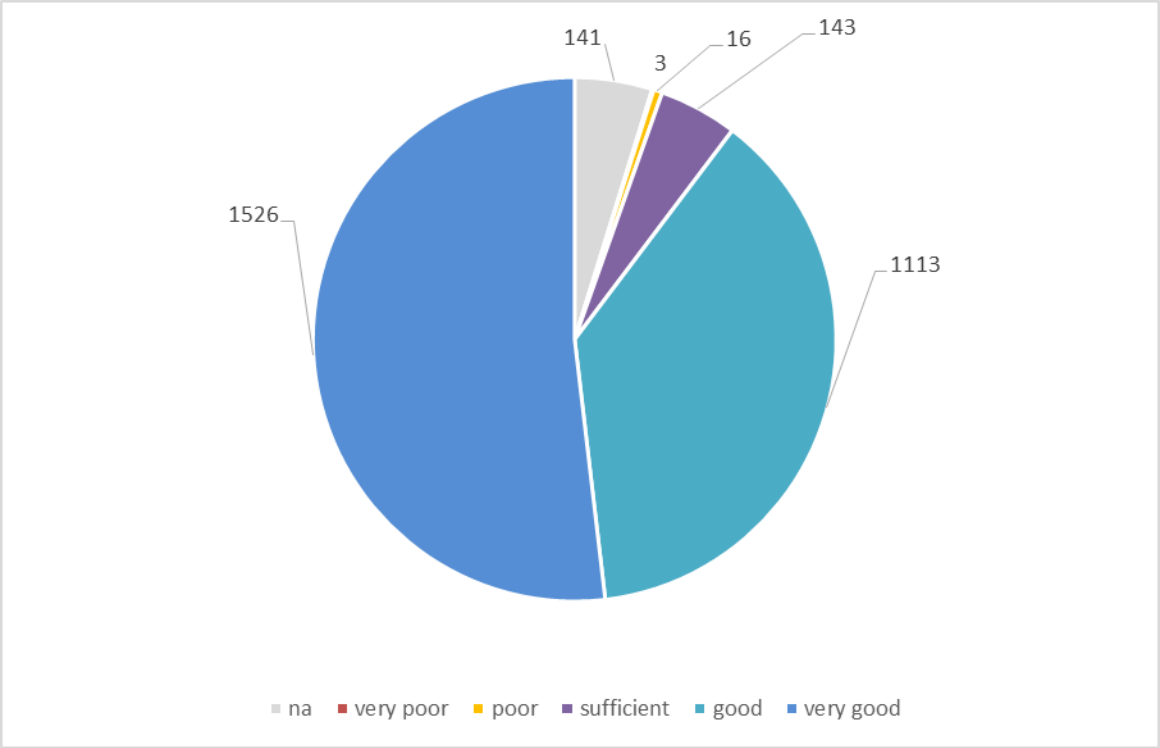


Figure 4: Overall results of the survey with external stakeholders

The details of results are shown in the following figures divided per Demonstration Activity (from [D8.2.1] and questions.

DA01	**Monitored System Overview**
1.1	Does the System show a correct network, topology and system inventory (comprehensive asset identification) ?
1.2	Is the network, topology and system inventory appropriate for the project's goals?
1.3	Is the network reconstruction showing useful geographical information?

Score			
na	3	1	1
1	0	1	1
2	1	0	0
3	3	3	3
4	35	33	28
5	50	54	59
mean	4,51	4,53	4,58
	DA01		
	1.1	**1.2**	**1.3**

DA02	**Monitored System Vulnerability Surface**
2.1	Does the System show a correct vulnerability inventory (correlation of assets to known vulnerabilities)?
2.2	Is the vulnerability inventory appropriate for the project's goals?

Score		
na	1	2
1	0	0
2	3	3
3	4	7
4	37	35
5	47	45
mean	4,41	4,36
	DA02	
	2.1	**2.2**

DA03	**Monitored System Mission Impact assessment**
3.1	Does the System show a correct view of the business processes of the Company, correlated with the dependent ICT/SCADA devices?
3.2	Is the view of the business processes and their relationship with the ICT/SCADA device appropriate for the project's goals?

Score		
na	3	3
1	0	0
2	0	1
3	6	4
4	32	34
5	50	50
mean	4,50	4,49
	DA03	
	3.1	**3.2**

DA04	**Risk Analysis, Proactive Risk and Attack Graph**
4.1	Does the System show a correct detection of the possible attack paths within the Monitored System, given a set of entrypoints?
4.2	Is the attack paths detection consistent with the network topology reconstruction?
4.3	Is the attack paths detection useful?
4.4	Does the System show a reconstruction of the quantification of the level of the Risk of the System?
4.5	Is the Risk quantification analysis appropriate for the project's goals?

Score					
na	4	4	3	5	4
1	0	0	0	0	0
2	0	0	0	0	0
3	3	2	1	8	6
4	32	30	27	35	34
5	53	56	61	44	48
mean	4,57	4,61	4,67	4,41	4,48
	DA04				
	4.1	**4.2**	**4.3**	**4.4**	**4.5**

DA05	**Strategic Response Overview**
5.1	Does the System show a prioritized strategic dashboard, with related strategic response plans optimized by risk reduction, response on financial investment impact evaluation and operational impact evaluation?

5.2	Is the strategic response plan computation consistent with the topology of the Monitored System and the quantification of the actual level of the Risk?
5.3	Is the strategic dashboard useful?

Score			
na	4	4	4
1	0	0	0
2	0	0	0
3	0	1	1
4	37	40	39
5	51	47	48
mean	4,58	4,52	4,53
	DA05		
	5.1	**5.2**	**5.3**

DA06	**Architecture Component Overview**
6.1	Is the software architecture of the PANOPTESEC coherent with the purposes of the Project?
6.2	Are the PANOPTESEC software security mechanisms (authentication, cryptography, etc.) providing an adequate protection for sensitive data?

Score		
na	2	9
1	0	0
2	0	0
3	1	8
4	36	40
5	53	35
mean	4,58	4,33
	DA06	
	6.1	**6.2**

DA07	Incident Correlation Overvew (IAP analysis)
7.1	Is the System able to correlate percieved security incidents with the computed attack paths?
7.2	Does the System visualize these correlation in order to alert the operator that a an attack is on going?
7.3	Is the System able to quantify the reactive level of the Risk, given a set of correlated incidents?

Score			
na	4	4	4
1	0	0	0
2	0	0	0
3	3	6	2
4	38	30	35
5	47	52	51
mean	4,50	4,52	4,56
	DA07		
	7.1	**7.2**	**7.3**

DA08	Tactical Response Plan
8.1	Does the System show a prioritize reactive dashboard, with related tactical response plans optimized by risk reduction and operational impact evaluation?
8.2	Are the tactical response plans coherent with the percieved correlated incidents?
8.3	Is the tactical dashboard useful?

Score			
na	5	5	6
1	0	0	0
2	0	0	0
3	2	4	2
4	36	38	26
5	49	45	58
mean	4,54	4,47	4,65
	DA08		
	8.1	**8.2**	**8.3**

Q01	**Do you think that the attack scenarios are realistic?**
Q02	**Do you think that the PANOPTESEC response time from a proactive perspective is appropriate?**
Q03	**Do you think that the PANOPTESEC response time from a reactive perspective is appropriate?**

Score			
na	7	6	7
1	0	0	0
2	1	0	1
3	5	9	5
4	28	33	39
5	51	44	40
mean	4,52	4,41	4,39
	Q01	**Q02**	**Q03**

Q04-Q5-Q6

Q04	**Is the graphical user interface appropriate for the project's goals?**
Q05	**Do you think that the PANOPTESEC or some part of the PANOPTESEC could be useful in your organization?**
Q06	**Does the system provide useful information?**

Score			
na	7	10	4
1	0	0	0
2	0	4	0
3	4	13	1
4	32	38	36
5	49	26	51
mean	4,53	4,06	4,57
	Q04	**Q05**	**Q06**

Q07-Q8-Q9

Q07	**Does the system provide up to date information?**
Q08	**Is the information clear?**
Q09	**Is the system easy to use?**

Score			
na	5	5	5
1	0	0	1
2	0	1	1
3	6	6	14
4	38	35	47
5	43	45	24
mean	4,43	4,43	4,06

The result of the survey states a general full appreciation of the PANOPTESEC System.

6.3.4 Conclusions

It is possible to state an overall satisfaction of the invited external stakeholders about the PANOPTESEC System. Each Operational Workshop lasted a sufficient time in order to allow them to have a detailed overview of the work and its capabilities and possible future exploitations. From a quantitative perspective, the total number of stakeholders involved and their direct affinity to cyber-security domain from different perspective gave the Consortium a very important feedback in terms of Validation of the PANOPTESEC System. In terms of traceability of the survey result with the System Level Requirements (as detailed in [D8.2.1]), it is possible to state that from an overall perspective these Requirements from [D2.2.1] have been validated by the external stakeholders, with a general overall satisfaction. This result enforces the Verification activities summarized within Section 3 and

4 of this report and the results from the first round of Workshops for the internal stakeholders.

7 PANOPTESEC SYSTEM DEPLOYMENT

7.1 Introduction

After the release of the [D7.4.1], the PANOPTESEC System has been packaged for the final installation within the Demonstration Environment in Acea (updated versions of some components may be installed during Month 36). While the Development and Testing Environment remain active in order to allow last bug-fixing and refinements of the prototype, a stable version, branched 23 September 2016 (main versions of the components, however, do not change from [D7.4.1] released), has been installed for the Operational Workshops activities.

7.2 Installation of the PANOPTESEC System Demonstration Prototype

The PANOPTESEC System Demonstration Prototype has been installed within 6 different Virtual Machine in the Deploy Environment. The Deployment Diagram in Figure 5 shows the current subdivision of the modules and their dependencies:

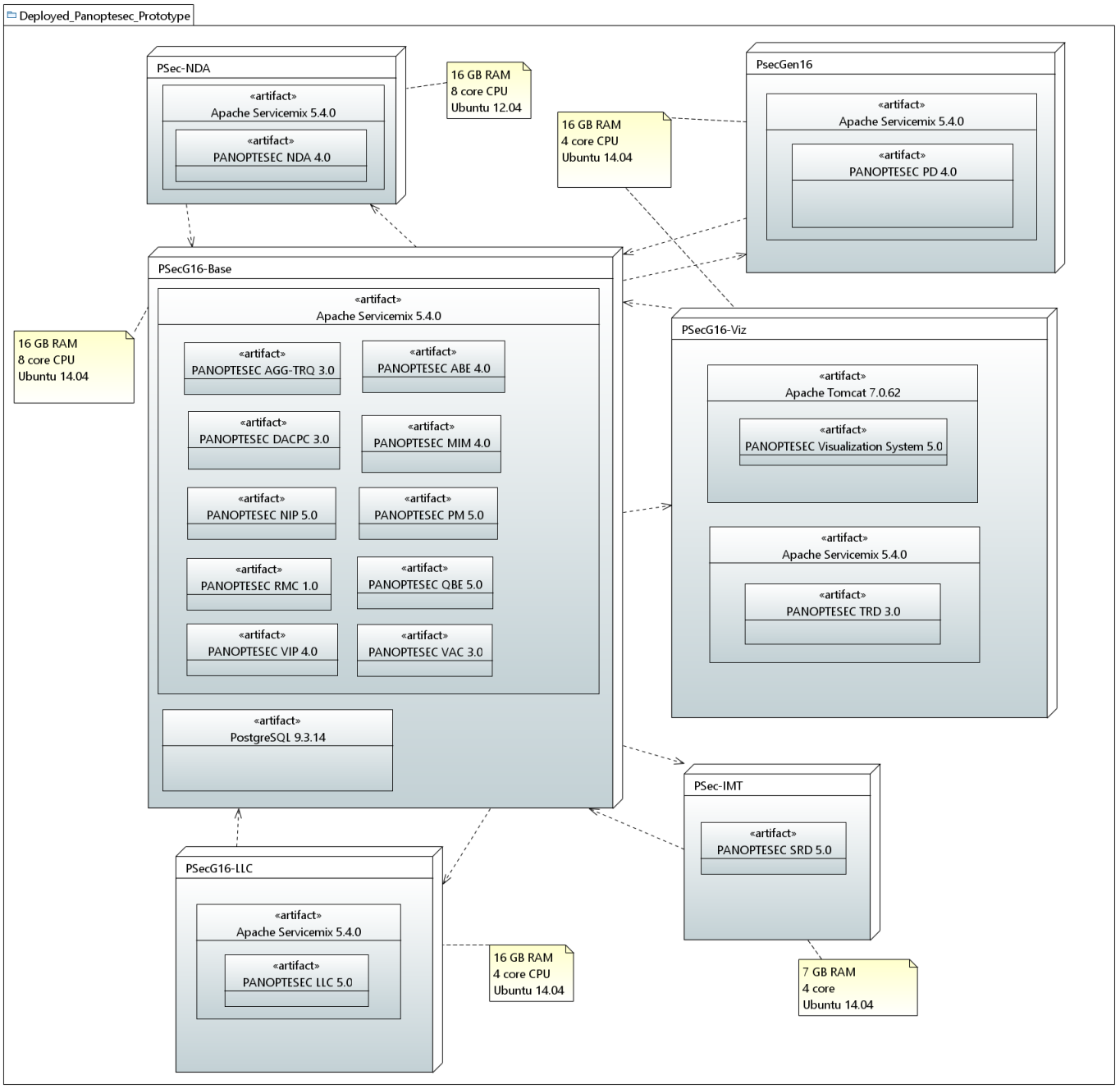


Figure 5: Installed Demonstration Prototype Deployment Diagram

In Table 8, the list of Virtual Machines, their main configuration details and the PANOPTESEC System installed software and components:

Table 8: Installed Demonstration Prototype resources description

VM Name	RAM	CPU (number of core)	Operating System	PANOPTESEC-related third party software	PANOPTESEC Components
PSecG16-BASE	16	8	Ubuntu 14.04	Apache Servicemix 5.4.0	AGG-TRQ v 3.0
					QBE v 5.0
					ABE v 4.0
					VAC v 3.0
					PM v. 5.0
				PostgreSQL 9.3.14	DACPC v 3.0
					NIP v 5.0
					MIM v 4.0
					VIP v 4.0
					RMC v 1.0
PSecG16-LLC	16	4	Ubuntu 14.04	Apache Servicemix 5.4.0	LLC v 5.0
PSec-NDA	16	8	Ubuntu 12.04	Apache Servicemix 5.4.0	NDA v 4.0
PSec-IMT	7	4	Ubuntu 14.04		SRD v 5.0
PSecGen16	16	4	Ubuntu 14.04	Apache Servicemix 5.4.0	PD v 4.0
PSecG16-Viz	16	4	Ubuntu 14.04	Apache Servicemix 5.4.0	TRD v 3.0
				Apache Tomcat 7.0.62	Visualization System v 5.1

In Figure 6, it is shown the Installed Demonstration System Prototype after the installation within the context of the Emulation Environment (PANOPTESEC System installed prototype is circled with a red rectangle):

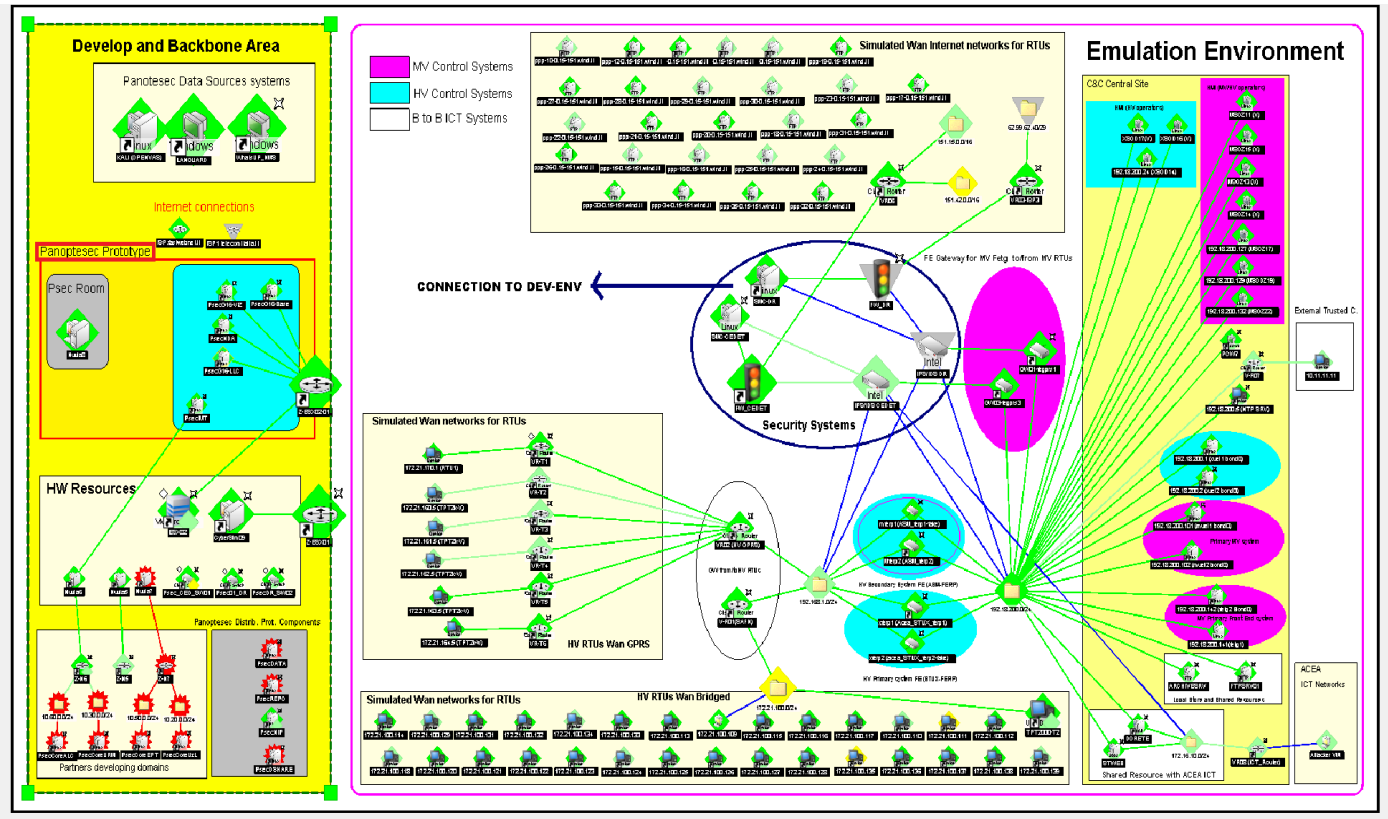


Figure 6: Installed PANOPTESEC Prototype within the context of the Emulation Environment

8 PANOPTESEC SYSTEM PERFORMANCES RESULTS

8.1 Introduction

The PANOPTESEC System has been carefully tested during the last months of development in order to assess the overall performances and scalability.

In terms of data sources, the Emulation Environment has been widely used, while the Production Environment results are depicted in Section 9.

All the following tests have been performed with the deployed PANOPTESEC System described in Section 7, with the exception of the test with a network wide around 8500 devices, where the main PANOPTESEC System VM has been provided with 24GB of ram (from 16).

8.2 Proactive chain

8.2.1 Monitored System data sources performances

In terms of tests over the proactive chain, it is important to assess the boundaries of the tests. Since the PANOPTESEC System is not a sensor or a scanner, it relies on the speed and accuracy of these data sources. The PANOPTESEC System is able to correlate and merge different data sources in order to optimize speed and results: for example, the current PANOPTESEC System deployment encompasses, as scanners data sources for the proactive chain:

- GFI Languard (asset management system)
- Whatsup Gold (network management system)
- Built-in topology scanner based on Nmap
- OpenVas vulnerability scanner

The combination of these scanners allows the PANOPTESEC System to perceive updates in the Monitored System with good timings:

GFI Languard performs a scan of the latest Emulation Environment (157 devices on 15 different broadcast domains) in 18500 seconds (as average): this is a deep scan, including inventory and vulnerabilities. Languard badly scales with the number of assets: a good solution could be to install multiple Languard on several VMs and make them scan over different broadcast domains (the PANOPTESEC System is able to manage multiple instances of Languard). In this case, however, it should be considered that licenses may become a non-trivial cost.

Whatsup Gold performs a scan of the latest Emulation Environment within 60 seconds, but the amount of information it receives is limited to basic topology (IP address, device on/off). It is very useful, however, in order to discover new devices and/or to check the status of the known devices. Whatsup Gold scales quite well with the size of the network.

The Consortium (while out of scope) developed and integrated a built-in topology scanner based on NMap (a widely-used topology scanner), with the aim of demonstrating that, with a fast data source, the PANOPTESEC System update time can scale quite well with the number of nodes.

The built-in scanner, called NetworkInventoryProcessorAgent, is able to perform a scan of the entire Emulation Environment within 950 seconds, allowing the PANOPTESEC System to perceive updates on ports (open/closed) within this amount of time. In terms of scalability, it scales very well, because all the processing is parallel with respect to the broadcast domains (more broadcast domain to scan, more threads. It may come a moment, of course, in which a new VM could be necessary).

Openvas vulnerability scanner performs a scan of the Emulation Environment in 7200 seconds (as average), which is actually the minimum perception time for new vulnerabilities/deployed patches. Also, Openvas does not scale well with the number of

nodes, but since it is free, it could be easily installed on multiple instances, if the number of devices grows up. The PANOPTESEC System is able to use multiple Openvas instances as data source.

As a conclusion, it is important to remember that data sources are NOT in the scope of the Project. The PANOPTESEC System, due to its general and optimized Data Model, is able to easily integrate many different data sources. If more performances are needed, a new data source should be considered.

8.2.2 Performances tests

The PANOPTESEC System proactive chain has been tested for several months, while its overall performances were improved constantly with the results of the tests. Within Table 9 it is possible to see the actual performances results of the PANOPTESEC System considering the latest version of the components and the System (23 September 2016).

These tests have been performed using the Emulation Environment (157 devices on 15 different broadcast domains with 576 vulnerabilities).

Both the Ontology based and the Java based Reachability Matrix Correlator have been tested on 5 different iterations of the Proactive Chain, from the beginning of the generation of the Network Inventory (first step of the proactive chain) to the generation of the Strategic Response Plans. The output from the 2 different RMCs is the same (although the Java version shrinks a bit the Json output, the content is equal).

These tests represent the performances of complete proactive chain, seen as a decision support for the Security Operator (a change in the Monitored System is perceived, the System computes all data and provides the Security Operator a set of possible Response Plans).

Within these tests, 3 hypothetic entry points on 3 different broadcast domains have been considered.

Table 9 Emulation Data proactive chain tests

Test	PANOPTESEC System with Ontology RMC (proactive chain computation time in seconds)	PANOPTESEC System with Java RMC (proactive chain computation time in seconds)
#1	880	292
#2	902	295
#3	920	298
#4	900	295
#5	928	300
Average	906	296

As can be seen, even using the slowest Reachability Matrix Correlator, proactive chain computation times for the Emulation Environment stay still on a reasonable number of seconds (within the boundaries of the Performance Requirements from [D2.2.1]). With the new RMC, however, the Consortium is very satisfied about the performances.

To these timings, it must be added from 10 to 20 seconds for the Graphical User Interface to be updated.

8.3 Reactive chain

8.3.1 Monitored System data sources performances

From a reactive perspective, the PANOPTESEC System receives a stream of SysLogs from the SMC manager collecting alerts from the security sensors of the Monitored System. In the context of the Emulation Environment, 2 firewalls and 2 IDS/IPS are installed and working.

While at Month 35 the normal rate of SysLogs received by the PANOPTESEC System was, as an average, of 50 SysLogs per second, scalability tests have been performed with a rate of 2000 SysLogs per second (by changing the configuration of the IDS/firewalls).

In terms of reactivity time of the security sensors (although it is not in the scope of the project, because the PANOPTESEC System is not a sensor), it has been verified that, on all tested attacks scenario described within [D8.2.1], SysLogs from the security sensors arrive to the PANOPTESEC System LLC component within 1 second (as an average. On some particular situations, e.g. when there is a huge network traffic, this time can increase up to 20 seconds) from the moment of the attack.

8.3.2 Performances tests

Reactive performance tests have been performed with the 3 attacks scenario described within [D8.2.1]. The overall behaviour of the System does not seem particularly affected by a specific attack scenario, hence the following tests will be related to the attack scenario 3.

Within Table 10 it is possible to see the actual performances results of the PANOPTESEC System considering the latest version of the components and the System (23 September 2016).

In order to analyse the reaction time of the System, it is important to state how fast is the correlation (which then displays to the operator the path which are currently under attack and the possible following path to be exploited) and how fast is the response time in terms of Tactical Response Plans to be proposed to the operator.

The first step of the attack scenario has been then repeated 5 times. Since the RMC is not directly involved in the reactive chain, reactive performances do not change depending on this component (Java based or Ontology based). Since many high-level alerts and Tactical Response Plans are sent during an attack, the next table shows an average of all alerts/response plan for each test.

Within these tests, 3 hypothetic entry points on 3 different broadcast domains have been considered.

Table 10 Emulation Data reactive chain tests

Test	PANOPTESEC System average reaction time in seconds (from SysLogs reception to alerts notification to the GUI)	PANOPTESEC System average reactive time in seconds (from SysLogs reception to Tactical Response Response Plans notification to the GUI)
#1	4.124	56
#2	4.067	64
#3	4.078	55
#4	4.130	53
#5	4.156	54
Average	4.111	56.4

As a conclusion, it can be seen that the PANOPTESEC System is able to quickly detect incoming exploits and signal them to the GUI (well under the maximum time imposed by the Performance Requirements). In terms of response computation, results are still acceptable and, as average, below 1 minute.

8.4 Scalability tests

8.4.1 Introduction

The PANOPTESEC System has been carefully tested using the Emulation Environment. It was interesting, however, to find analytical methods in order to evaluate the performances with an higher number of devices on several broadcast domains. In order to cope with that, the Network Inventory Processor component has been enriched with a submodule able to replicate (and then, assign correct IP addresses) all nodes of an existing broadcast domain, applications and vulnerabilities included (in addition, other vulnerabilities can be analytically added to several devices in order to increase the computation times), and connect it with a proper IP Interface of a router.

It was then possible to simulate bigger networks: since all PANOPTESEC System components depend on the Network Inventory created by NIP, being these devices “real” or “simulated” did not change nothing for the rest of the System in terms of computation time.

8.4.2 1250 Nodes tests

Following the concepts from Section 8.4.1, the PANOPTESEC System has been tested with 1257 devices with 5045 vulnerabilities.

Both the Ontology based and the Java based Reachability Matrix Correlator have been tested on 5 different iterations of the Proactive Chain, from the beginning of the generation of the Network Inventory (first step of the proactive chain) to the generation of the Strategic

Response Plans. The output from the 2 different RMCs is the same (although the Java version shrinks a bit the Json output, the content is equal).

These tests depict the performances of complete proactive chain, seen as a decision support for the Security Operator (a change in the Monitored System is perceived, the System computes all data and provides the Security Operator a set of possible Response Plans).

Within these tests, 3 hypothetic entry points on 3 different broadcast domains have been considered.

Table 11 1257 nodes tests

Test	PANOPTESEC System with Ontology RMC (proactive chain computation time in seconds)	PANOPTESEC System with Java RMC (proactive chain computation time in seconds)
#1	3580	421
#2	3595	415
#3	3640	430
#4	3623	410
#5	3656	419
Average	3618	419

As can be seen, using the slowest Reachability Matrix Correlator, proactive chain computation times for 1257 devices stay barely around the boundaries of the Performance Requirements from [D2.2.1], one hour. With the new RMC, however, the Consortium is very satisfied about the performances: from 157 devices to 1257 the computation times augmented by less than 150 seconds.

To these timings, it must be added from 20 to 70 seconds for the Graphical User Interface to be updated (some of the views are slower than other).

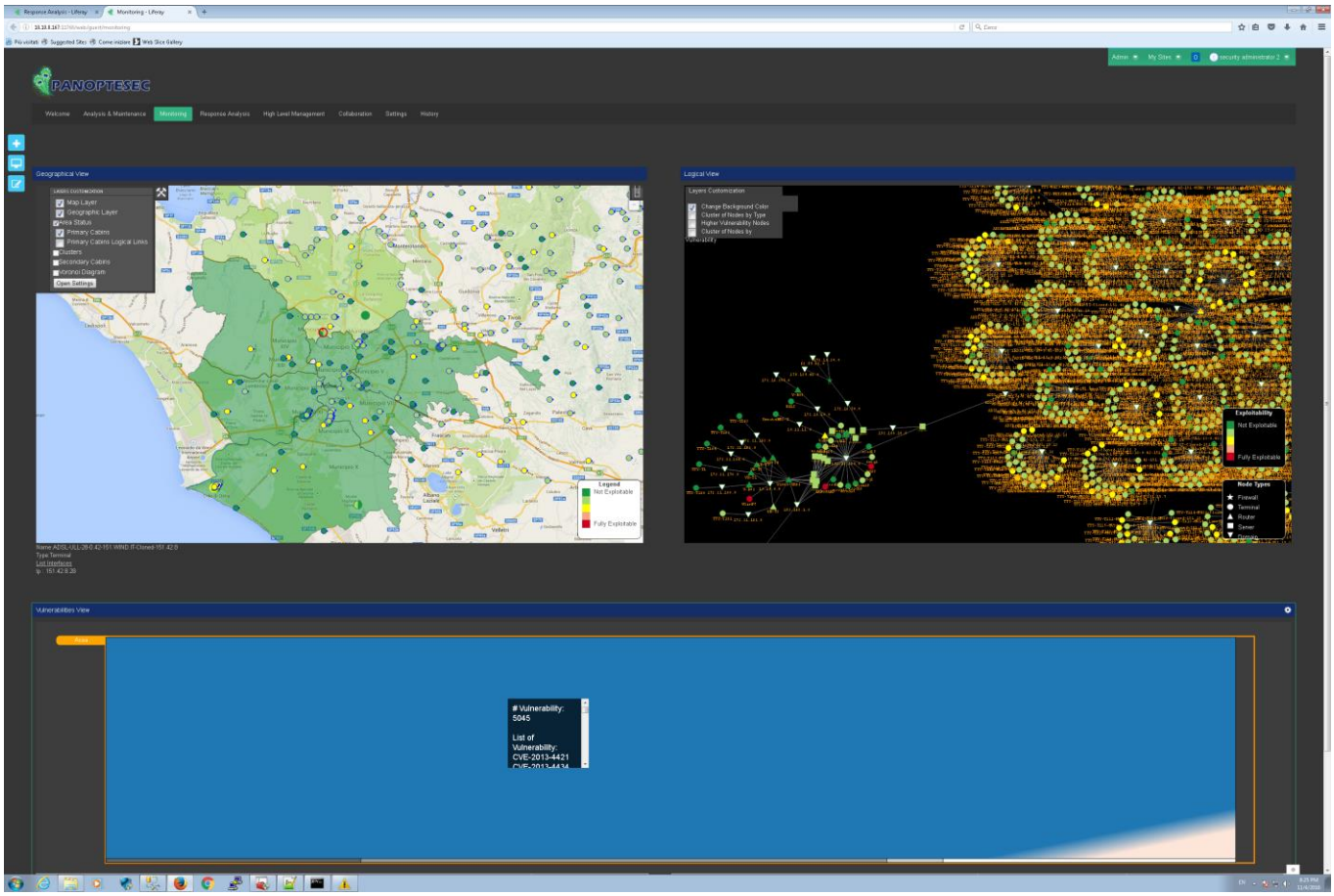


Figure 7: Analysis and Maintenance view with 1250 nodes

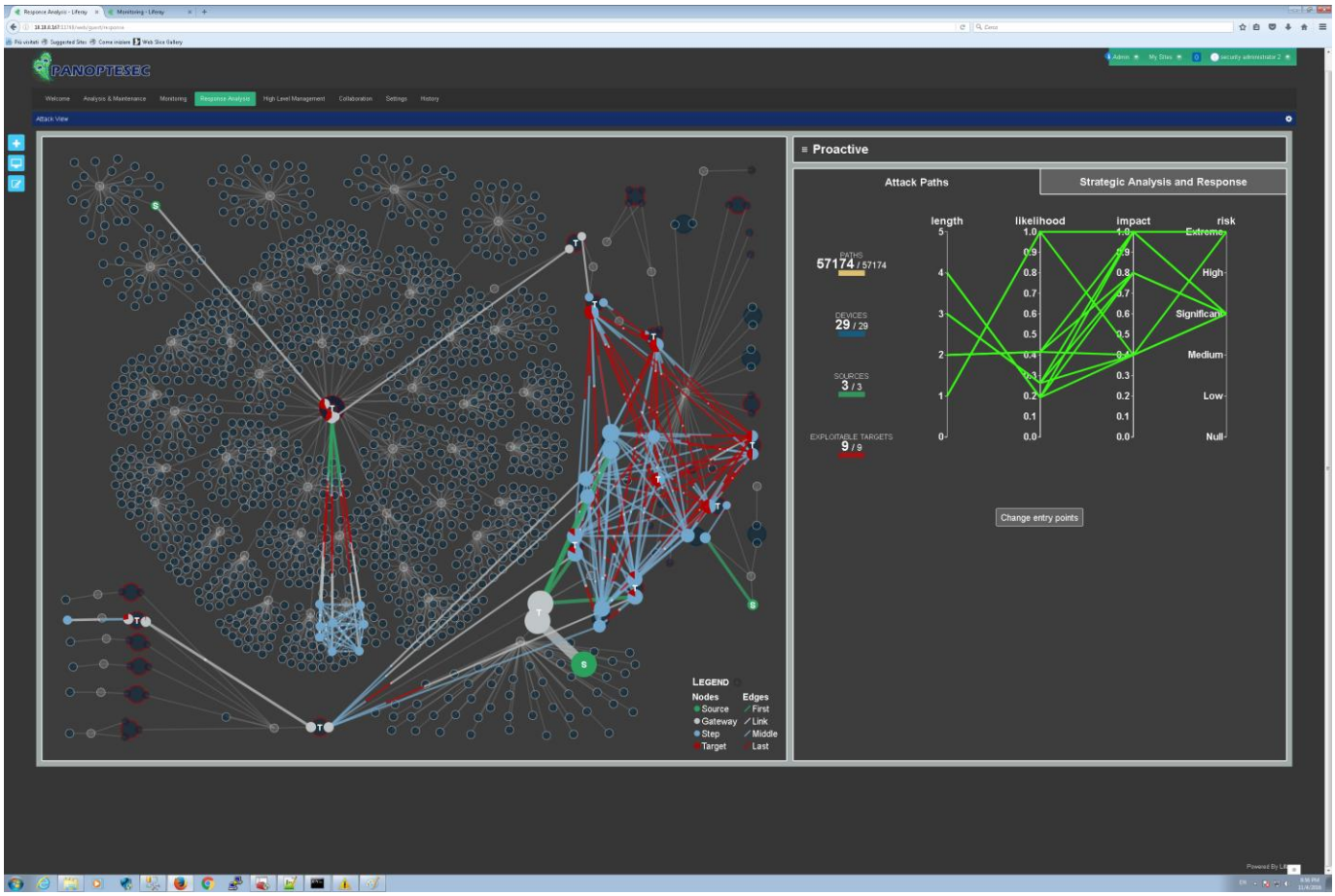


Figure 8 Proactive view with 1250 nodes

8.4.3 3000 Nodes tests

Following the concepts from Section 8.4.1, the PANOPTESEC System has been tested with 2907 devices with 11766 vulnerabilities.

Only the Java based Reachability Matrix Correlator has been tested on 5 different iterations of the Proactive Chain, from the beginning of the generation of the Network Inventory (first step of the proactive chain) to the generation of the Strategic Response Plans. The Ontology based Reachability Matrix Correlator already reached its limit with the tests in Section 8.4.2.

These tests depict the performances of complete proactive chain, seen as a decision support for the Security Operator (a change in the Monitored System is perceived, the System computes all data and provides the Security Operator a set of possible Response Plans).

Within these tests, 3 hypothetic entry points on 3 different broadcast domains have been considered.

Table 12 3000 nodes tests

Test	PANOPTESEC System with Java RMC (proactive chain computation time in seconds)

#1	594
#2	598
#3	609
#4	610
#5	604
Average	603

With the new RMC the Consortium is very satisfied about the performances: from 157 devices to 2907 the computation times just doubled.

With a network this size, it has been possible to observe that the PANOPTESEC System main installation reaches up to 10GB of allocated ram, during the computations (it is reaching its boundaries of 16 GB of ram).

To these timings, it must be added from 20 to 140 seconds for the Graphical User Interface to be updated (some of the views are a bit heavy).

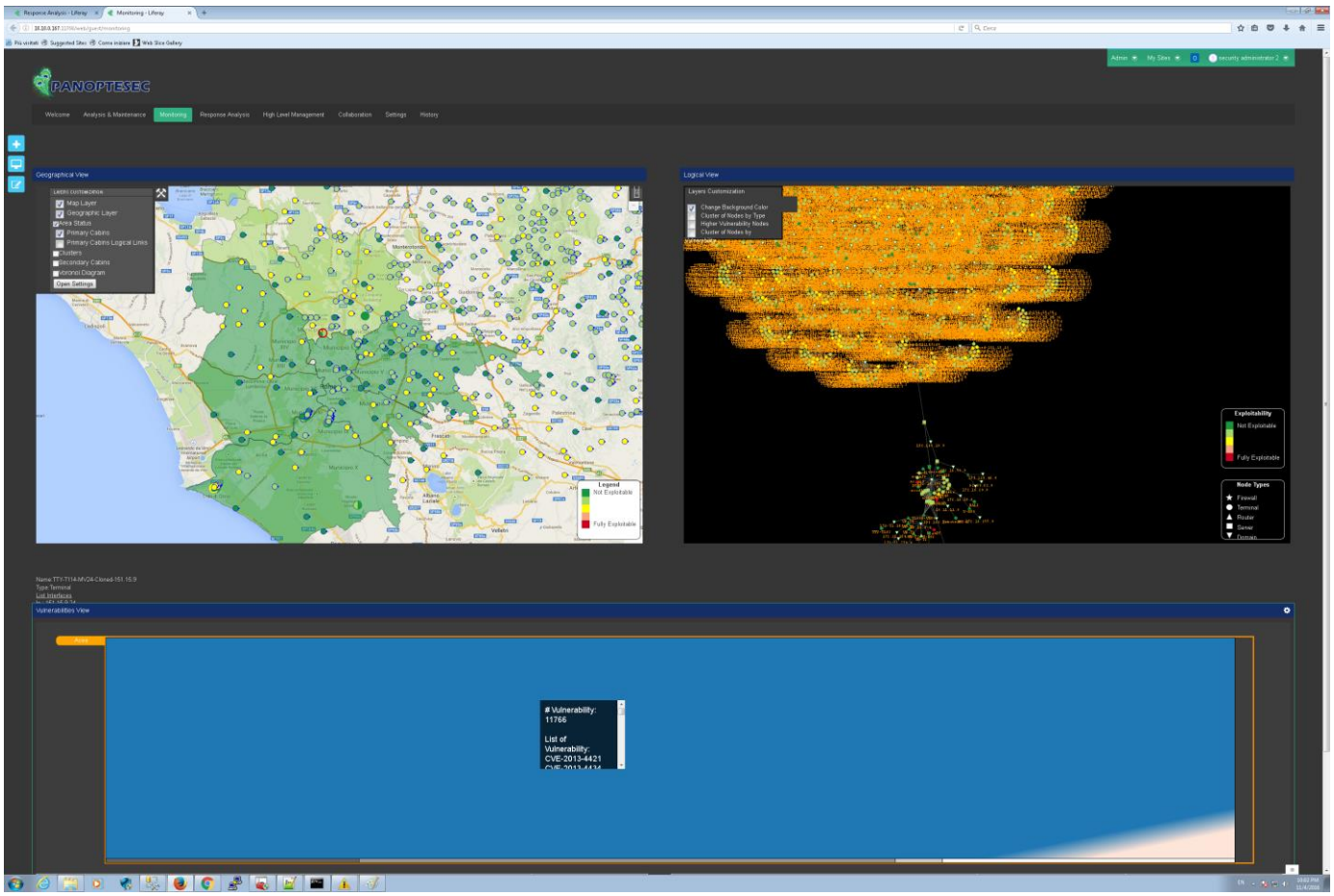


Figure 9 Analysis and Maintenance view with 3000 nodes

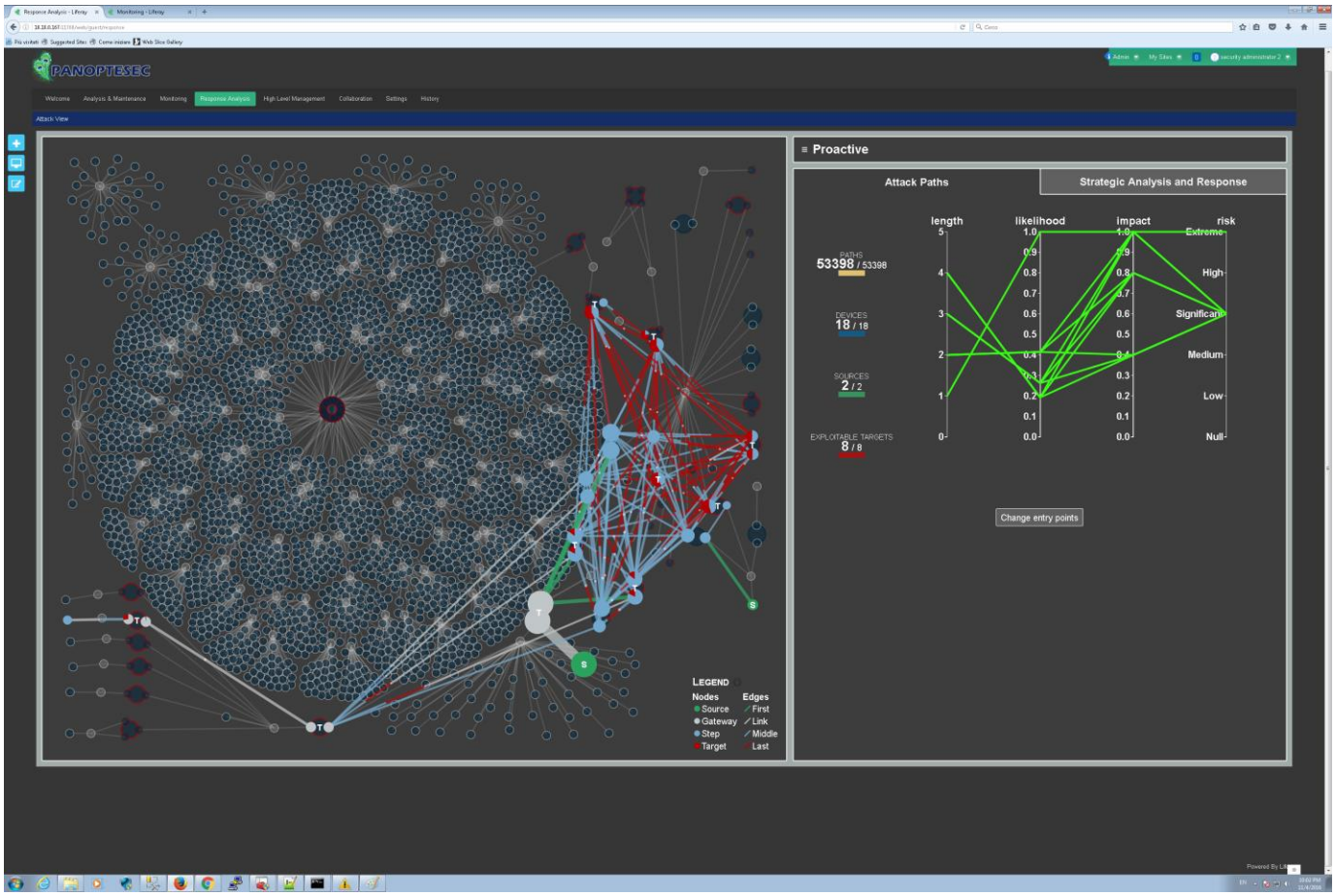


Figure 10 Proactive view with 3000 nodes

8.4.4 8500 Nodes tests

Following the concepts from Section 8.4.1, the PANOPTESEC System has been tested with 8407 devices with 28545 vulnerabilities.

Only the Java based Reachability Matrix Correlator has been tested on 5 different iterations of the Proactive Chain, from the beginning of the generation of the Network Inventory (first step of the proactive chain) to the generation of the Strategic Response Plans. The Ontology based Reachability Matrix Correlator already reached its limit with the tests in Section 8.4.2.

These tests depict the performances of complete proactive chain, seen as a decision support for the Security Operator (a change in the Monitored System is perceived, the System computes all data and provides the Security Operator a set of possible Response Plans).

Within these tests, 3 hypothetic entry points on 3 different broadcast domains have been considered.

Table 13 8500 nodes tests

Test	PANOPTESEC System with Java RMC (proactive chain computation time in seconds)

#1	967
#2	950
#3	988
#4	976
#5	982
Average	973

With the new RMC, the Consortium is very satisfied about the performances: from 157 devices to 8407 the computation times just tripled.

With a network this size, WP7 had to add 8 GB of ram to the main VM and other 6 GB of ram to the VM managing the Strategic Response Decider.

To these timings, it must be added from 20 to 240 seconds for the Graphical User Interface to be updated (some of the views are a bit heavy).

Due to the limited space of the views for such a number of nodes, it is possible to see that many of them collapse in the same position of the screen.

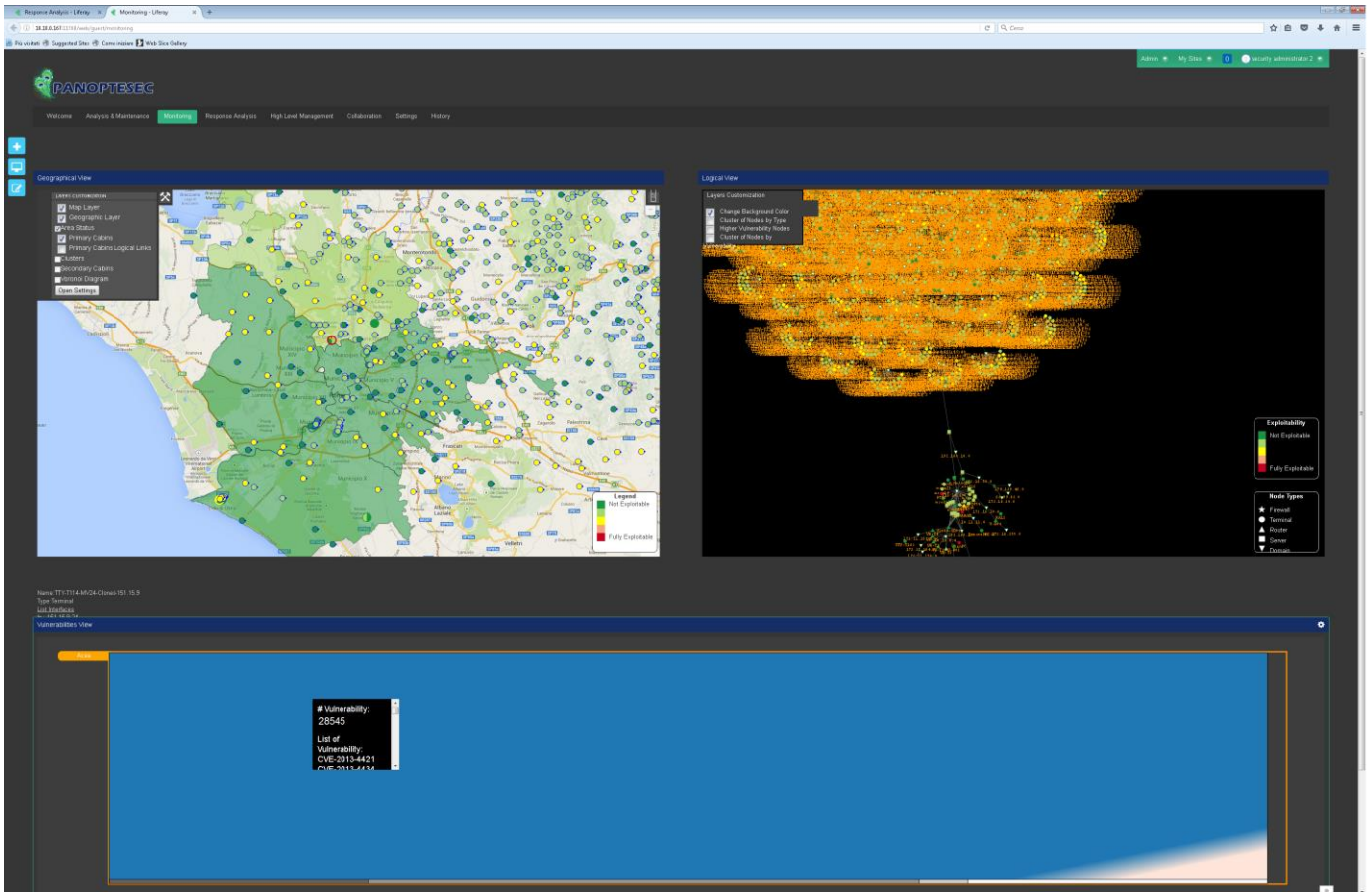


Figure 11 Analysis and Maintenance view with 8500 nodes

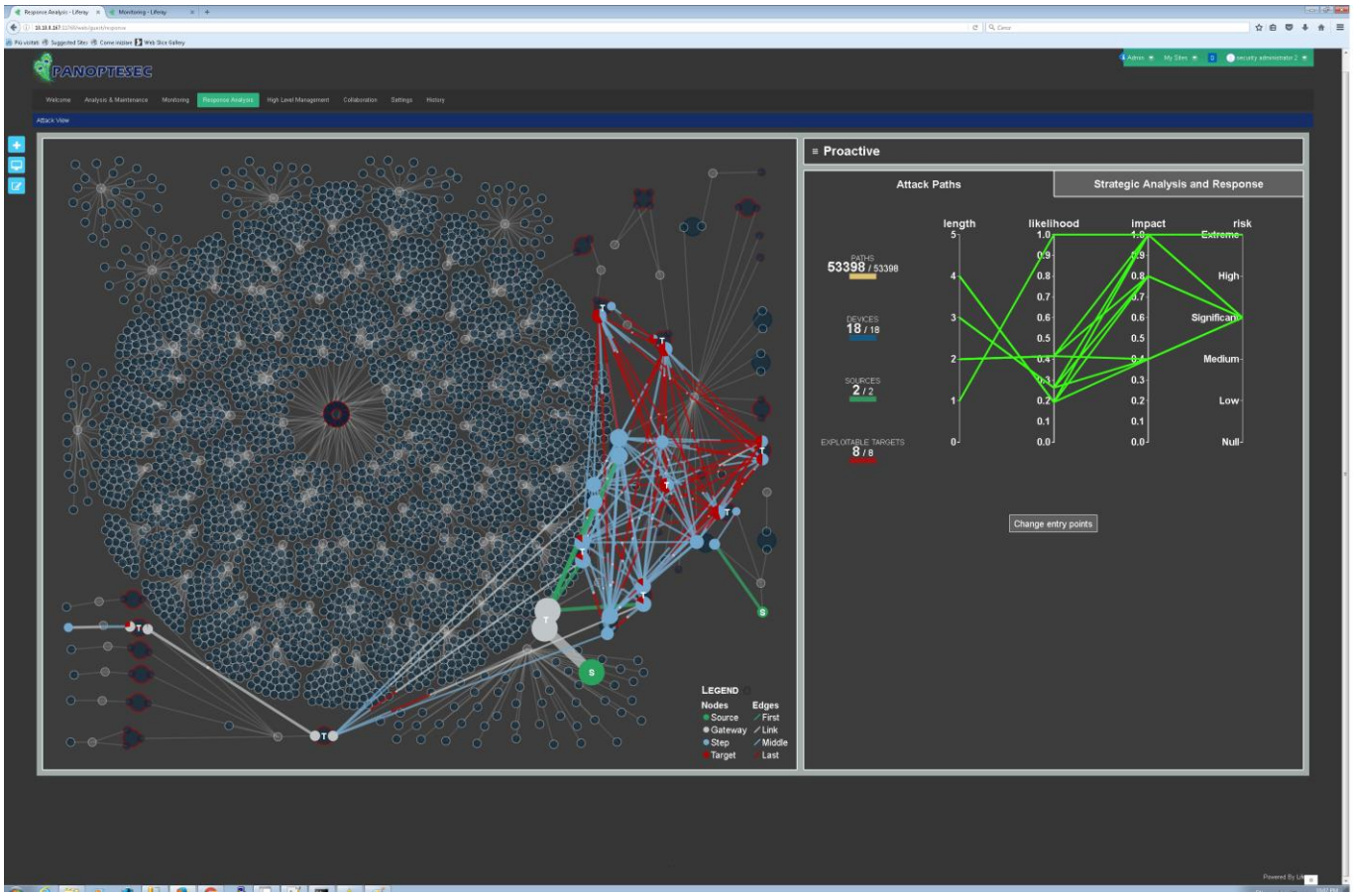


Figure 12 Proactive View with 8500 nodes

8.4.5 Conclusions

The PANOPTESEC System seems able to scale with the size of the network. Other tests with around 10000 nodes had been carried out: some more ram needs to be added. Except for that, and of course longer computation times (but always well under the Performance Requirements limits), the System is able to scale. On an industrial version for very big networks, however, some reengineering of the source code of the components may be needed, in order to increase their performances. In addition, the GUI should be modified in order to be able to cluster group of devices and limit then the overhead on the browser.

9 PANOPTESEC SYSTEM PRODUCTION DATA TESTS

9.1 Introduction

The Emulation Environment developed for the PANOPTESEC System is described within [D7.1.1] and has been built in order to allow the Consortium develop and test the system on a close copy of an operational environment (in this case, the command and control network of Acea Areti), without the constraints of a critical production system (which would have

made the development completely impossible. The command and control network of Acea Areti manages high and medium voltage distribution for six million people and many industries, and each issue or malfunctioning may cause millions of euros of damage.

Considering that, it would have been impossible to freely analyse, scan, compromise, understand the network with the aim of building and testing and experiment the System, especially from a reactive perspective). Most of the tests described within Section 4 have been conducted with data from the Emulation Environment, able to reconstruct the topology of the command and control centre in terms of the critical elements and its main boundaries in terms of security sensors and external connections. Due to the fact that the Emulation Environment has been built using a combination of original devices from the Disaster Recovery site of Acea Areti (equal to the servers within the production environment) and of virtual clones of the remaining devices of the production environment, real SCADA traffic is flowing within the emulated network.

All high-voltage distribution RTUs from the production environment have been cloned and virtualized, allowing a constant SCADA communication with the SCADA server, their proxies and the HMI operator devices. Due to the high affinity with the production environment, Acea Areti will use the Emulation Environment as a complex and complete testbed (with a security focus: for example, it will be used for penetration testing against the command and control centre) during the next years.

The produced Emulation Environment is then very close to the production environment at the time of the network and security assessment of October 2014 (of course, also due to the inputs from the PANOPTESEC Project, the actual production environment shows new different elements mostly connected with the intent of extending the cyber security defences).

In order to be able to show that the PANOPTESEC System is also able to work on a production environment, WP7 organized a set of tests using production environment data, both from a proactive and a reactive perspective.

9.2 Proactive chain tests with production data

In order to test the PANOPTESEC System with production data, it was necessary to perform scans of the Production Environment of the Command and Control environment of Acea Areti.

These scans have been performed on 27/04/2016, 07/05/2016 and 18/07/2016.

Acea Areti uses, within its Production Environment, the same Asset Management System the PANOPTESEC Consortium uses for the Emulation Environment (GFI Languard). Openvas vulnerability scanner it is used for additional information about vulnerabilities of the assets.

Since two of the data source are the same of the Emulation Environment, it is possible to relatively easily use these scanners results offline within the PANOPTESEC Testing Environment (actually deployed PANOPTESEC System VMs, described in Section 7.2) have been cloned and used for the Production Data tests.

It must be noted that, even if the complete High and Medium Voltage IP Network of Acea Areti counts around 6000 devices, only 183 are under direct analysis of the scanners (Command and Control centre and the High Voltage RTUs). These devices have been then considered by our tests.

Due to the affinity with the Emulation Environment, the PANOPTESEC System fed with production data did not have to be configured with different information about critical assets and firewalling rules, since these assets are the same on both environments. WP7 just had to check the routing tables for the nodes which are not present into the Emulation Environment (from the network and vulnerabilities assessment performed by the Consortium at October 2014, Acea Areti renewed partially the Command and Control network, adding several devices -HMI stations, routers, IDS and IPS).

The PANOPTESEC System have been tested with the 3 different scans mentioned before, using the latest versions of the components and the System (23 September 2016). This report analyses the results from the last scan (using the latest versions of the components).

Both the Ontology based and the Java based Reachability Matrix Correlator have been tested on 5 different iterations of the Proactive Chain, from the beginning of the generation of the Network Inventory (first step of the proactive chain) to the generation of the Strategic Response Plans. The output from the 2 different RMCs is the same (although the Java version shrinks a bit the Json output, the content is equal).

Within these tests, 3 hypothetic entry points on 3 different broadcast domains have been considered.

Table 14 Production Data proactive chain tests

Test	PANOPTESEC System with Ontology RMC (proactive chain computation time in seconds)	PANOPTESEC System with Java RMC (proactive chain computation time in seconds)
#1	770	220
#2	781	223
#3	775	222
#4	769	220
#5	776	222
Average	774.2	221.4

As can be seen, even using the slowest Reachability Matrix Correlator, proactive chain computation times for the Production Environment stay still on a reasonable number of seconds (within the boundaries of the Performance Requirements from [D2.2.1]). With the new RMC, however, the Consortium is very satisfied about the performances, even with the data from the Production Environment.

It is interesting to see that, even if the Production Environment contains a highest number of devices with respect to the Emulation Environment, PANOPTESEC System performs slightly better with the former (in particular, with the Ontology based Reachability Matrix Correlator). This is due to three main reasons:

- Data sources for the Emulation Environment are 4, while the Production Environment has only 2 data sources available for the proactive chain. Correlation times are then slower with Emulation Environment data (and, of course, the Emulation Environment data sources give more detailed data);
- The Production Environment has less exploitable vulnerabilities with respect to the Emulation Environment (due to the network and vulnerability assessment performed in order to build the Emulation Environment, several devices have been patched in the Production Environment during the last 2 years. Less exploitable vulnerabilities mean less attack paths to be calculated and less computation time taken by the Strategic Response Decider);
- While similar to the Production Environment, the Emulation Environment has a more complex topology: a set of devices have been added with the purpose of adding complexity to the computation.

9.3 Reactive chain tests with production data

The production environment reactive test was conducted on 19th July 2016 and started at 10:22:40 and ended on 17:41:51.

Since the PANOPTESEC System reactive chain is based on the results from the proactive chain, the reactive components have been fed with the latest results, from a proactive chain perspective, of the Production Environment (Network Inventory, Vulnerability Inventory, Scored Vulnerability Inventory, Reachability Matrix, Attack Graph, Proactive Risk Profile).

The Low-Level Correlator component of the PANOPTESEC System was successfully deployed, listening directly the SysLog messages coming from the production SMC security manager, collecting all logs from IPS, IDS and firewalls. Due to the affinity between the Emulation Environment and the Production Environment (IPS, IDS and firewalls in production are just updated versions of the same elements within the Emulation. Within the last 2 years, however, also due to the results of the PANOPTESEC Project, ACEA Areti increased the total number of security devices for its Production Environment. The amount of SysLog is hence greatly superior with respect to the Emulation Environment. From this consideration, even if the format of the data received is the same, a scalability test was useful in order to discover the boundaries of the reactive system in terms of receiving and processing raw messages from the security devices), the LLC component was able to receive production SysLogs with no adaptation.

During the testing hours, an overall of 6,769,533 Syslog messages were received. Due to the criticality of the Production Environment, IPS and FWs are used to block unexpected attempts of communication. This procedure is referred to as white listing. Therefore, as is to

be expected, no LLC alerts were produced (LLC could not match any incident raising a possible alert to the High Level Online Correlator, as expected). However, LLC demonstrated to be able to sustain the rate of incoming Syslog messages within the production environment.

The test then lasted for 26340 seconds: as an average, LLC received and processed 257 messages per seconds.

It could be observed, however, that on some particular moments of the day the number of messages received raised substantially, due to internal shifting weekly maintenance procedures (the specific day of the test was chosen exactly for this reason, in order to stress the reactive system to its boundaries using the Production Environment during what it is considered the most critical moment in terms of traffic).

Considering the test from 15:27:49 to 17:41:51, LLC received 5,988,271 Syslog messages (while the peak was between 16:00 to 17:00).

Within 8042 seconds then, LLC received and processed an average of 744 messages per second, with peaks around 9000 messages per second. Memory consumption and CPU allocation was far under the limits (at the peak, LLC and its Integration Framework bundle were occupying 25% CPU, from 2 to 4 GB of ram during the peaks. Configuration of the VM for the Production Environment test was the same as the usual installation for the Emulation Environment).

As can be seen, the Production Environment test was useful in order to:

- Demonstrate that the PANOPTESEC System could be easily deployed within the Production Environment, and sustain its rate of incidents from the security sensors;
- Demonstrate that the PANOPTESEC System can receive and process up to 9000 incidents per second (this result could not be proven with the Emulation Environment, which is able to generate up to 2000 incidents per second), while merging and correlating the messages with the Network Inventory;
- Based on this, for the LLC as a standalone component (without the Integration Framework bundle, hence choosing a lighter – and less reliable of course – integration mechanism with the rest of the PANOPTESEC System), processing up to 10,000 alerts per second on average can be easily achieved. However, deploying the LLC in an environment with 100,000 alerts per second, or more, is considered high risk.

10 CONCLUSIONS

10.1 Significant results achieved

This deliverable shows that the implemented *Demonstration System Prototype* of the PANOPTESEC System is verified against a) the High Level Design proposed in [D3.1.2] (and already verified in [D7.2.2R], [D7.3.1R], [D7.4.1R], [D4.2.2R], [D4.3.1R], [D5.2-3.3R], [D5.4.1R], [D6.2.2R] and [D6.3.1R]; and is verified against b) the System Level Functional and

Non-Functional requirements from [D2.2.1]. Interactions between components are verified against the Low-Level Design.

Several Validation activities have been performed during Months 35 and 36, with very good results: the Operational Workshops have been a success, in terms of number and quality of the attendees and in terms of surveys results.

The PANOPTESEC System has been carefully tested in order to evaluate the performances, which are good (well under the Performance Requirements limits), especially considering that it is a prototype, not a product.

Some tests with the Production Environment validated that the System could be installed easily in this environment and provide useful information to the operators.

10.2 Deliverable validation

This deliverable has been validated in accordance with the quality assurance plan of the PANOPTESEC project as outlined in the [PH15] and following supporting quality review procedures.

11 REFERENCES

[D2.1.1] PANOPTESEC consortium, *"Deficiency Evaluation", Project deliverable D2.1.1*, Version 1.0, 28.04.2014

[D2.2.1] PANOPTESEC consortium, *"Operational Requirements", Project deliverable D2.2.1*, Version 2.1, 27.03.2015

[D3.1.2] PANOPTESEC consortium, *"System High Level Design", Project deliverable D3.1.2*, Version 2.0, 27.03.2015

[D4.1.1] PANOPTESEC consortium, *"Data Collection and Correlation Requirements", Project deliverable D4.1.1*, Version 2.0, 27.03.2015

[D4.2.2] PANOPTESEC consortium, *"Data Collection and Correlation Components Prototypes II", Project deliverable D4.2.2,* Version 1, 31.10.2015

[D4.2.2R] PANOPTESEC consortium, *"Data Collection and Correlation Components Prototypes II, Verification Report", Project deliverable D4.2.2,* Version 1, 06.04.2016

[D4.3.1] PANOPTESEC consortium, *"Data Collection and Correlation Integration Prototype", Project deliverable D4.3.1,* Version 1, 30.06.2016

[D4.3.1R] PANOPTESEC consortium, *"Data Collection and Correlation Integration Prototype Verification Report", Project deliverable D4.3.1,* Version 1, 30.06.2016

[D5.1.1] PANOPTESEC consortium, *"Response System for Dynamic Risk Management Requirements", Project deliverable D5.1.1*, Version 2.1, 27.03.2015

[D5.1.2] PANOPTESEC consortium, *"Response System for Dynamic Risk Management Models and High-Level Design", Project deliverable D5.1.2*, Version 1.0, 31.10.2014

[D5.2-3.3] PANOPTESEC consortium, *"Proactive/Reactive Response System Components Prototypes II", Project deliverable D5.3.3, D5.2.3,* Version 1, 31.10.2015

[D5.2-3.3R] PANOPTESEC consortium, *"Proactive/Reactive Response System Components Prototypes II, Verification Report", Project deliverable D5.3.3, D5.2.3,* Version 1, 06.04.2016

[D5.4.1] PANOPTESEC consortium, *"Response System for Dynamic Risk Management Integration Prototype", Project deliverable D5.4.1,* Version 1, 30.06.2016

[D5.4.1R] PANOPTESEC consortium, *"Response System for Dynamic Risk Management Integration Prototype Verification Report", Project deliverable D5.4.1,* Version 1, 30.06.2016

[D6.2.2] PANOPTESEC consortium, *"Visualization System Components Prototypes II", Project deliverable D6.2.2,* Version 1, 31.10.2015

[D6.2.2R] PANOPTESEC consortium, *"Visualization System Components Prototypes II, Verification Report", Project deliverable D6.2.2,* Version 1, 06.04.2016

[D6.3.1] PANOPTESEC consortium, *"Visualization System Integration Prototype", Project deliverable D6.3.1,* Version 1, 30.06.2016

[D6.3.1R] PANOPTESEC consortium, *"Visualization System Integration Prototype Verification Report", Project deliverable D6.3.1,* Version 1, 30.06.2016

[D7.1.1] PANOPTESEC consortium, *"Simulation Environment", Project deliverable D7.1.1,* Version 1, 31.10.2014

[D7.2.2] PANOPTESEC consortium, *"Integration Framework Prototype II", Project deliverable D7.2.2,* Version 1, 31.10.2015

[D7.2.2R] PANOPTESEC consortium, *"Integration Framework Prototype II Verification Report", Project deliverable D7.2.2,* Version 1, 06.04.2016

[D7.3.1] PANOPTESEC consortium, *"Integration Framework Prototype II", Project deliverable D7.3.1,* Version 1, 30.06.2016

[D7.3.1R] PANOPTESEC consortium, *"Integration Framework Prototype II Verification Report", Project deliverable D7.3.1,* Version 1, 30.06.2016

[D7.4.1] PANOPTESEC consortium, *"Demonstration System Prototype", Project deliverable D7.4.1,* Version 1, 31.08.2016

[D7.4.1R] PANOPTESEC consortium, *"Demonstration System Prototype Verification Report", Project deliverable D7.4.1,* Version 1, 31.08.2016

[D7.4.2] PANOPTESEC consortium, *"Demonstration System Prototype Report", Project deliverable D7.4.2,* Version 1, 31.10.2016

[D8.2.2] PANOPTESEC consortium, *"Installed Demonstration System Prototype", Project deliverable D8.2.2,* Version 1, 30.09.2016

[D8.2.2R] PANOPTESEC consortium, *"Installed Demonstration System Prototype Verification Report", Project deliverable D8.2.2,* Version 1, 30.09.2016

[IEEE-STD-610] The Institute of Electrical and Electronics Engineers (IEEE), *"IEEE Standard Glossary of Software Engineering Terminology"*, *IEEE Std 610.12-1990*, 28.09.1990

[PH15] PANOPTESEC consortium, *"PANOPTESEC Project Handbook", Project internal document,* version 0.1, 27.03.2015

12 ANNEX A – PANOPTESEC SYSTEM HIGH LEVEL DESIGN

The complete actual High Level Design for the PANOPTESEC System (and its associated Low Level Design focusing on the actually implemented components can be found in the [D7.4.1] deliverable. Here a summary is reported.

As a reminder, the PANOPTESEC System is composed by several sub-systems:

- Data Collection and Correlation Subsystem
- Dynamic Risk Management Response subsystem
- Visualization subsystem

All of them are glued by the Integration Framework.

12.1 Data Collection and Correlation sub-system

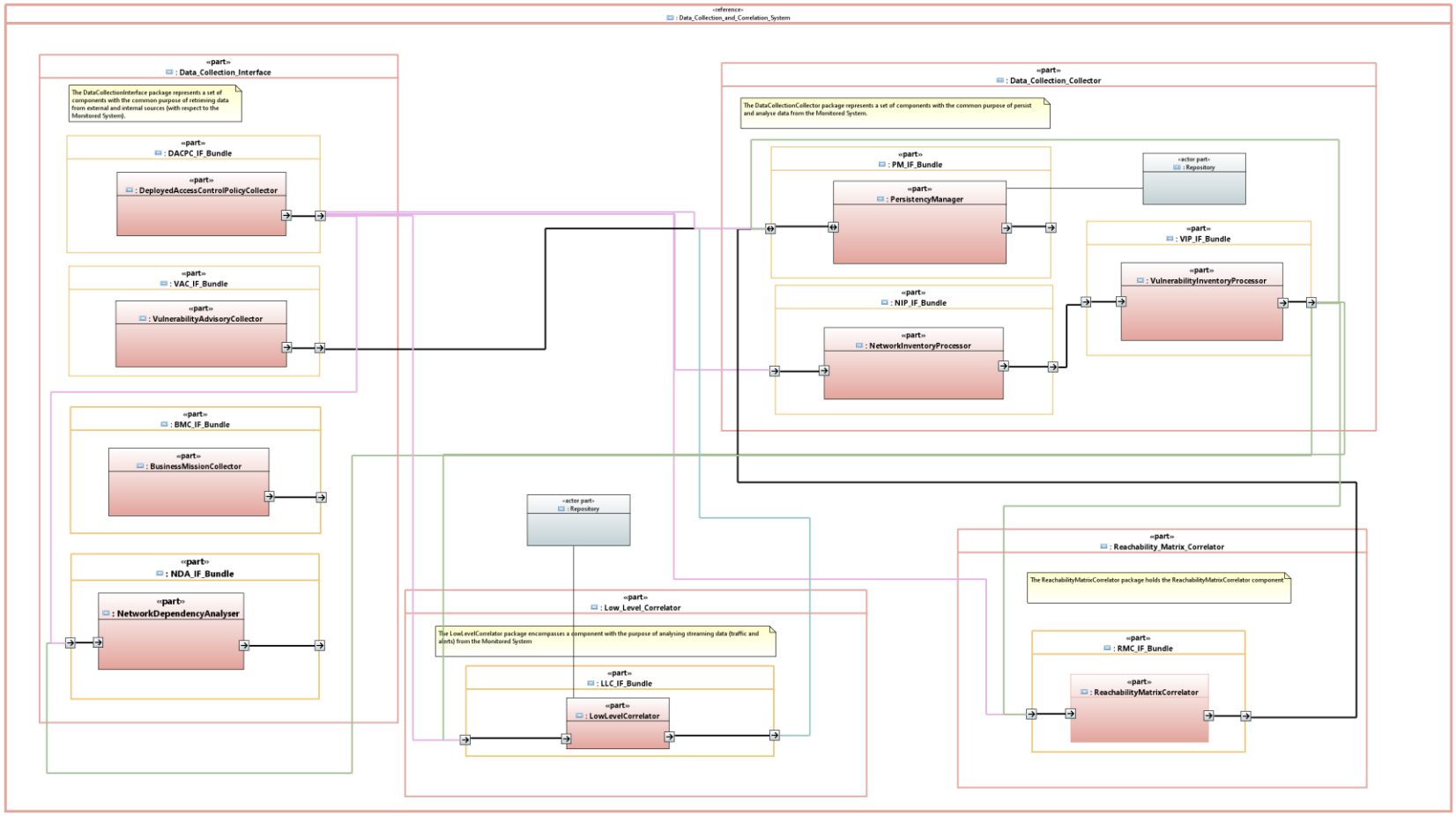


Figure 13 Data Collection and Correlation Sub-System High Level Design Logic overview

12.1.1 Data Collection Interface package Logic View

In the actual Design, the Data Collection Interface package encompasses these components:

- DeployedAccessControlPolicyCollector
- VulnerabilityAdvisoryCollector
- BusinessMissionCollector
- NetworkDependencyAnalyser

Next Figure depicts a higher level of detail on the DCI package:

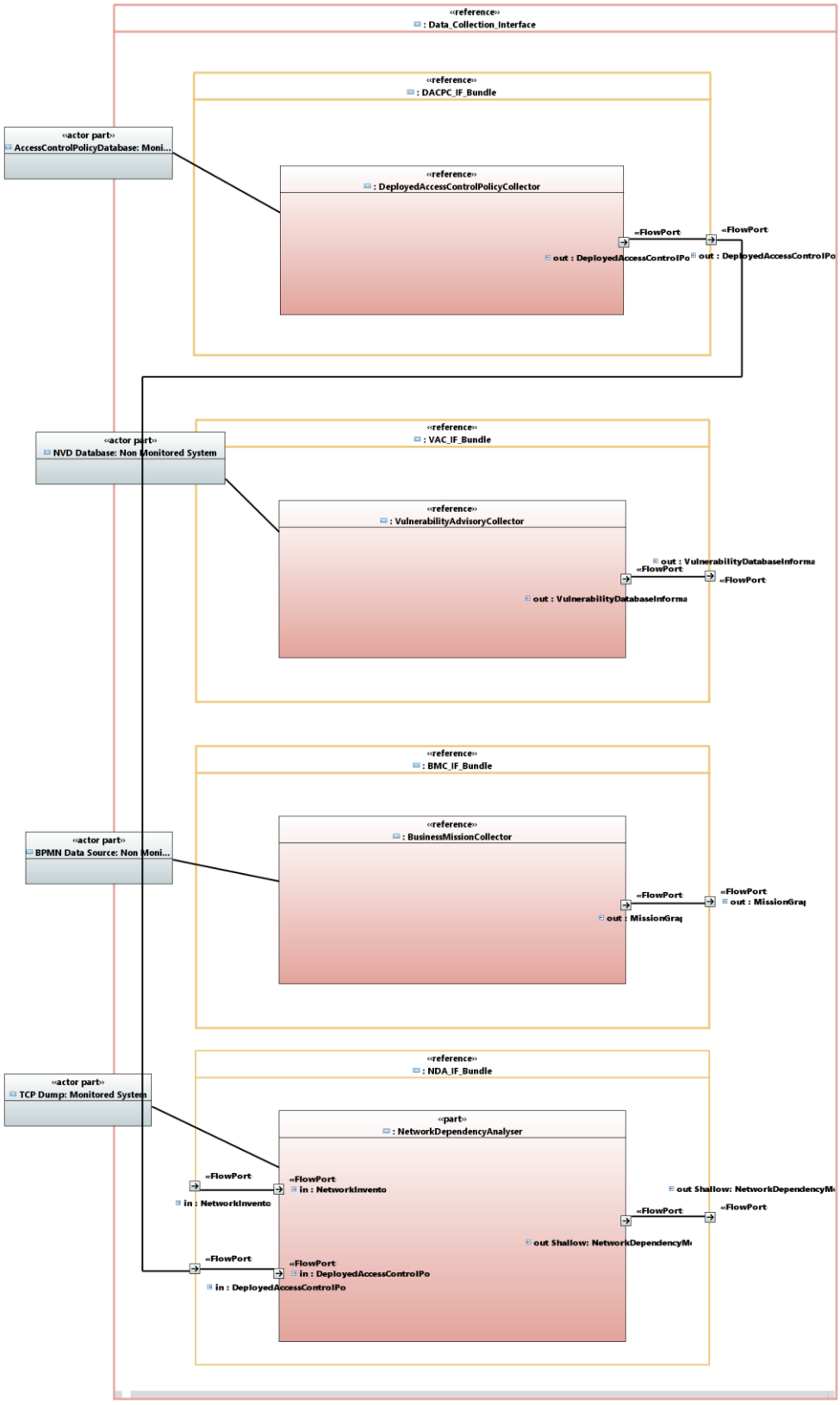


Figure 14 Data Collection Interface package Logic View

12.1.2 Data Collection Collector package Logic View

In the actual Design, the Data Collection Collector package encompasses these components:

- PersistencyManager
- NetworkInventoryProcessor
- VulnerabilityInventoryProcessor

Next Figures depict a higher level of detail on the DCC package:

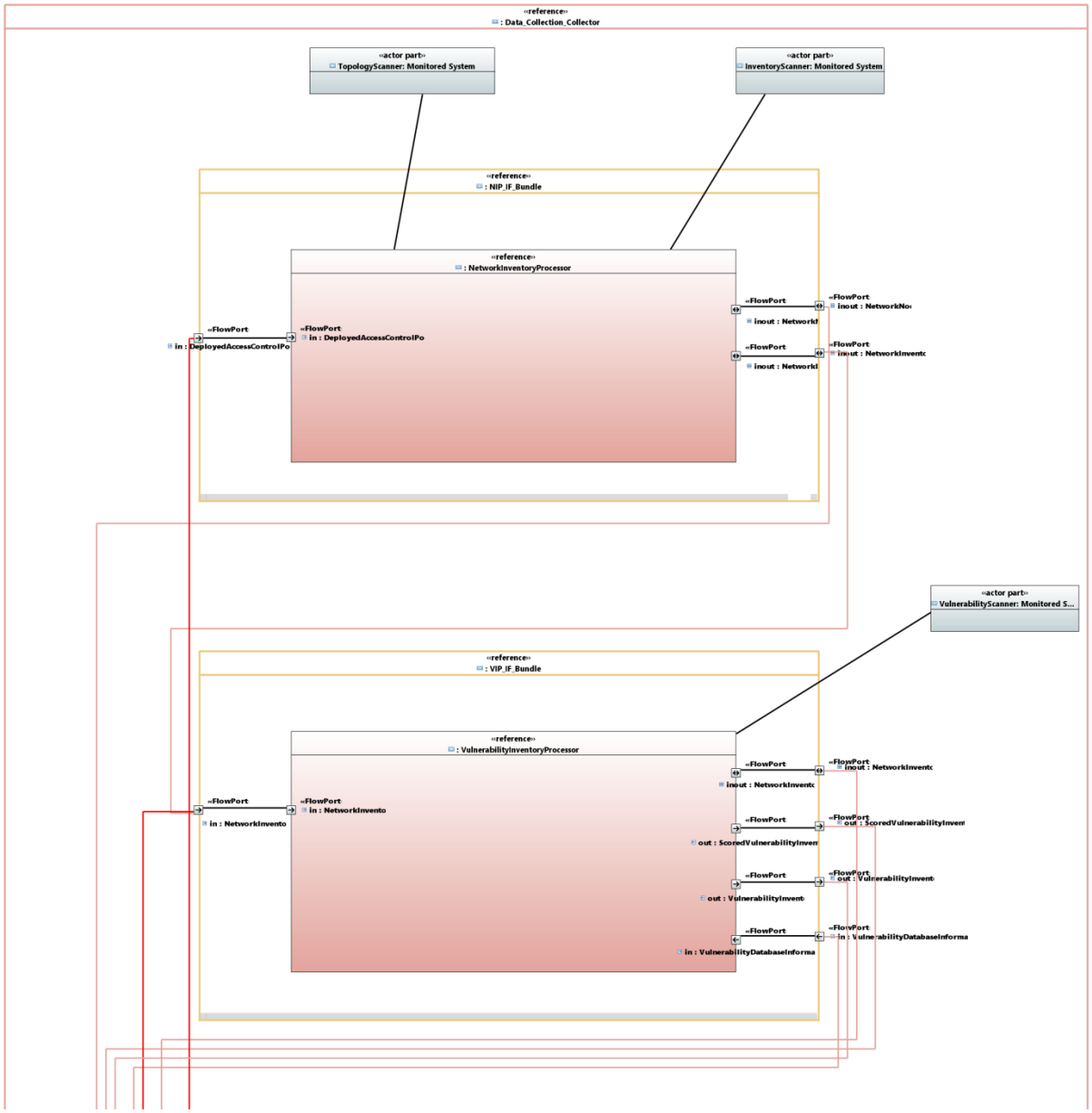


Figure 15 Data Collection Collector package Logic View

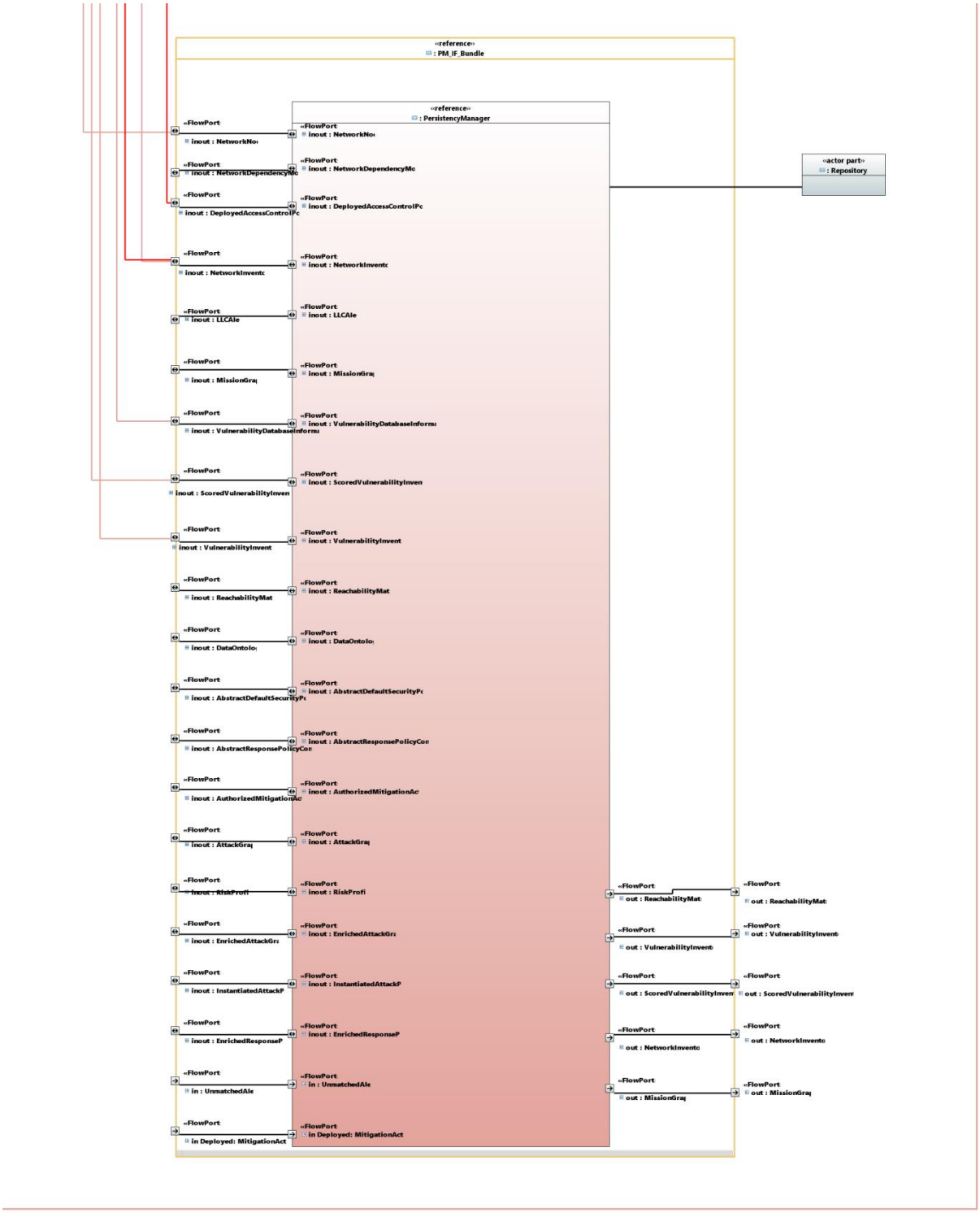


Figure 16 Data Collection Collector package Logic View

12.1.3 Low Level Correlator package Logic View

In the actual Design, the Low Level Correlator package encompasses this component:

- LowLevelCorrelator

Next Figure depicts a higher level of detail on the LLC package:

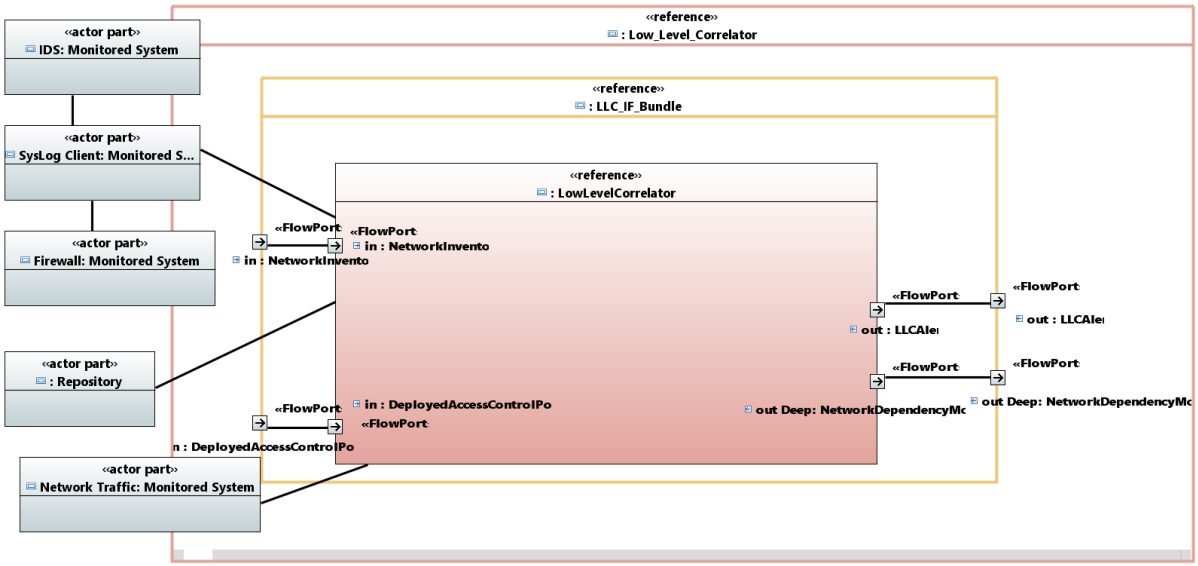


Figure 17 Low Level Correlator package Logic View

12.1.4 Reachability Matrix Correlator package Logic View

In the actual Design, the Reachability Matrix Correlator package encompasses this component:

- ReachabilityMatrixCorrelator

Next Figure depicts a higher level of detail on the RMC package:

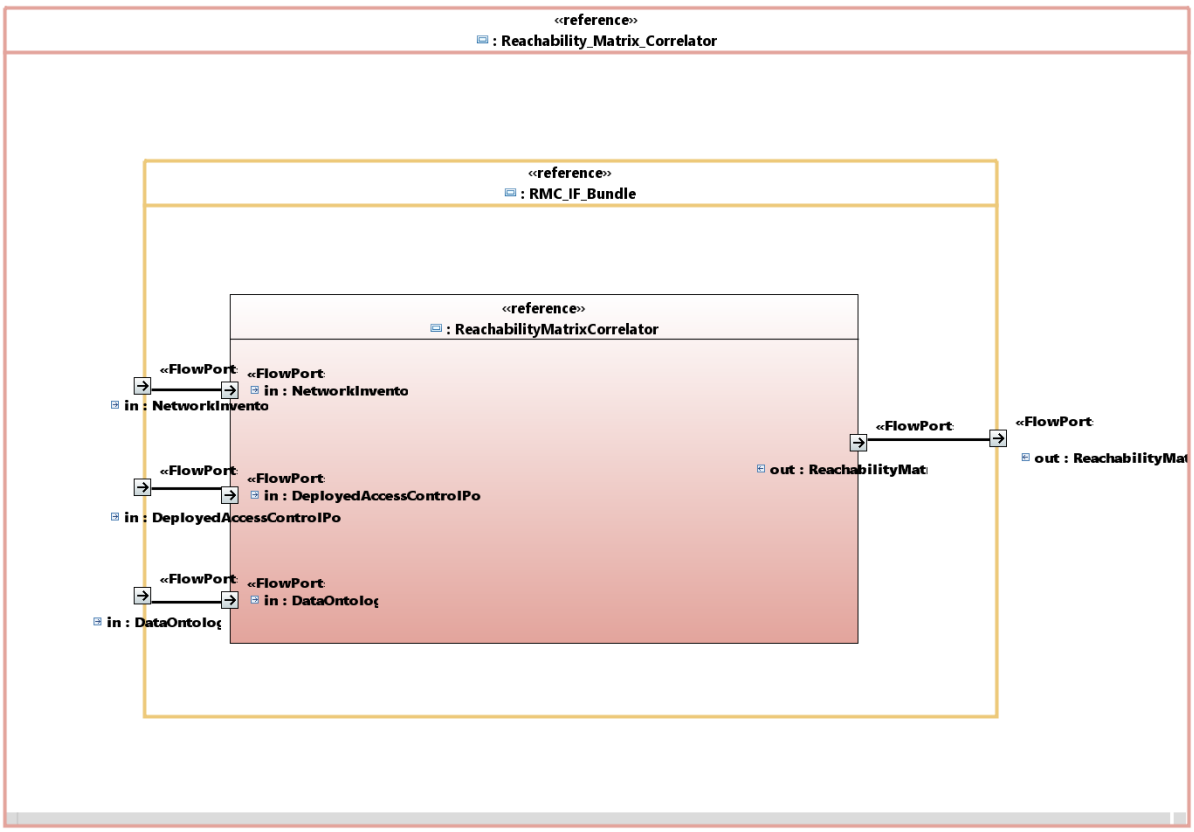


Figure 18 Reachability Matrix Correlator package Logic View

12.1.5 Mission Impact Module package Logic View

In the actual Design, the Mission Impact Module package encompasses this component:

- MissionImpactModule

Next Figure depicts a higher level of detail on the MIM package:

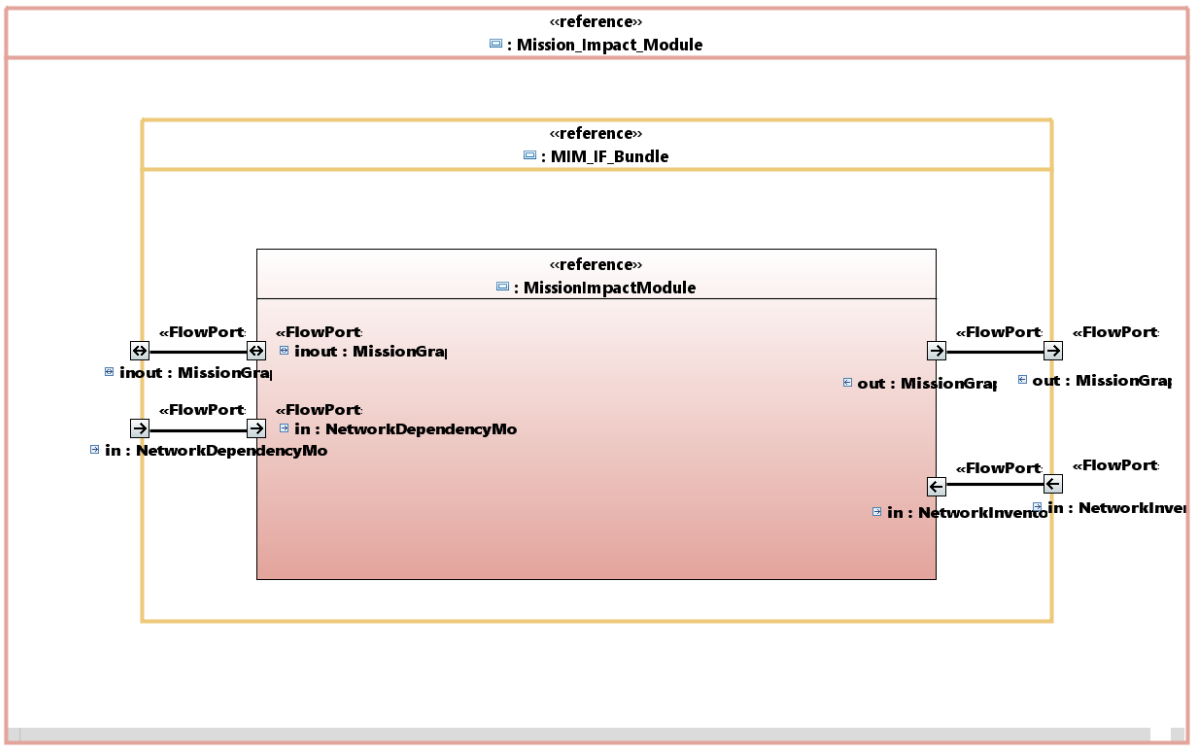


Figure 19 Mission Impact Module package Logic View

12.3 Dynamic Risk Management Response sub-system

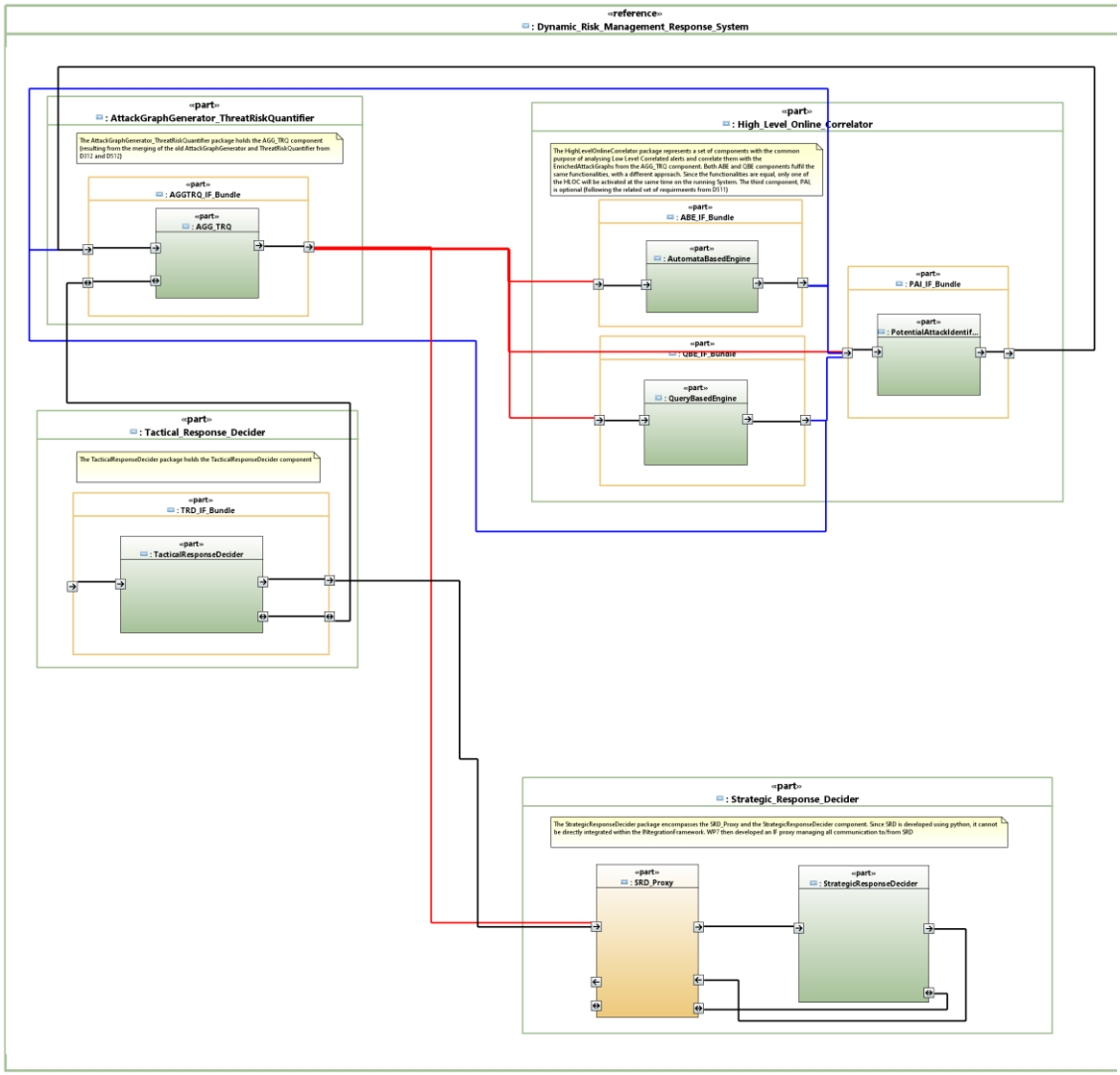


Figure 20 Dynamic Risk Management Response Sub-System High Level Design Logic overview

12.3.1 AGG-TRQ package Logic View

In the actual Design, the AGG-TRQ component (inside the logic package of the AttackGraphGenerator-ThreatRiskQuantifier) has been created from the merging of the [D3.1.2] AttackGraphGenerator and RiskQuantifier components.

Next Figure depicts a higher level of detail on the AttackGraphGenerator-ThreatRiskQuantifier package:

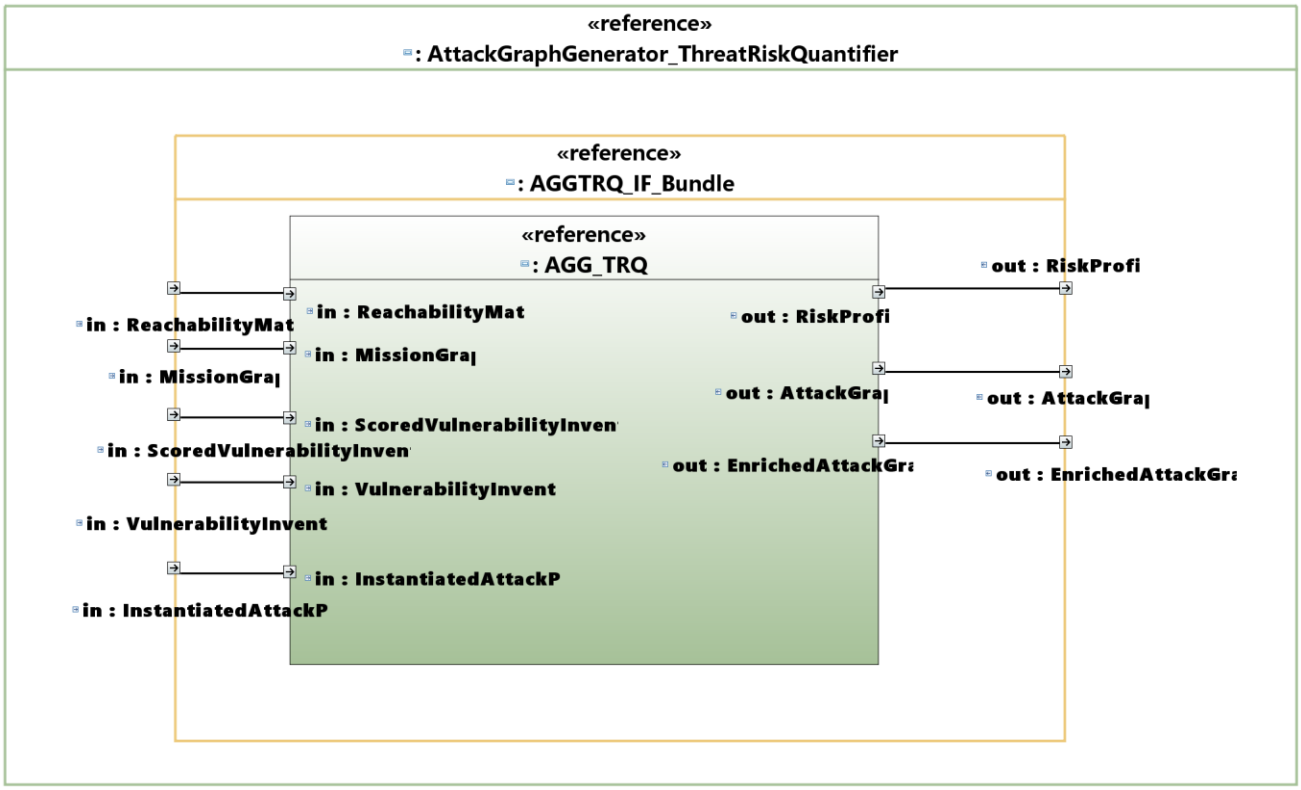


Figure 21 AGG-TRQ package Logic View

12.3.2 Strategic Response Decider package Logic View

The Strategic Response Decider package encompasses the StrategicResponseDecider component and its proxy (since the SRD cannot be directly integrated within the Integration Framework, because it is developed in Python language –and the Integration Framework works with Java components- a proxy has been developed, in order to allow the rest of the PANOPTESEC System to communicate with it).

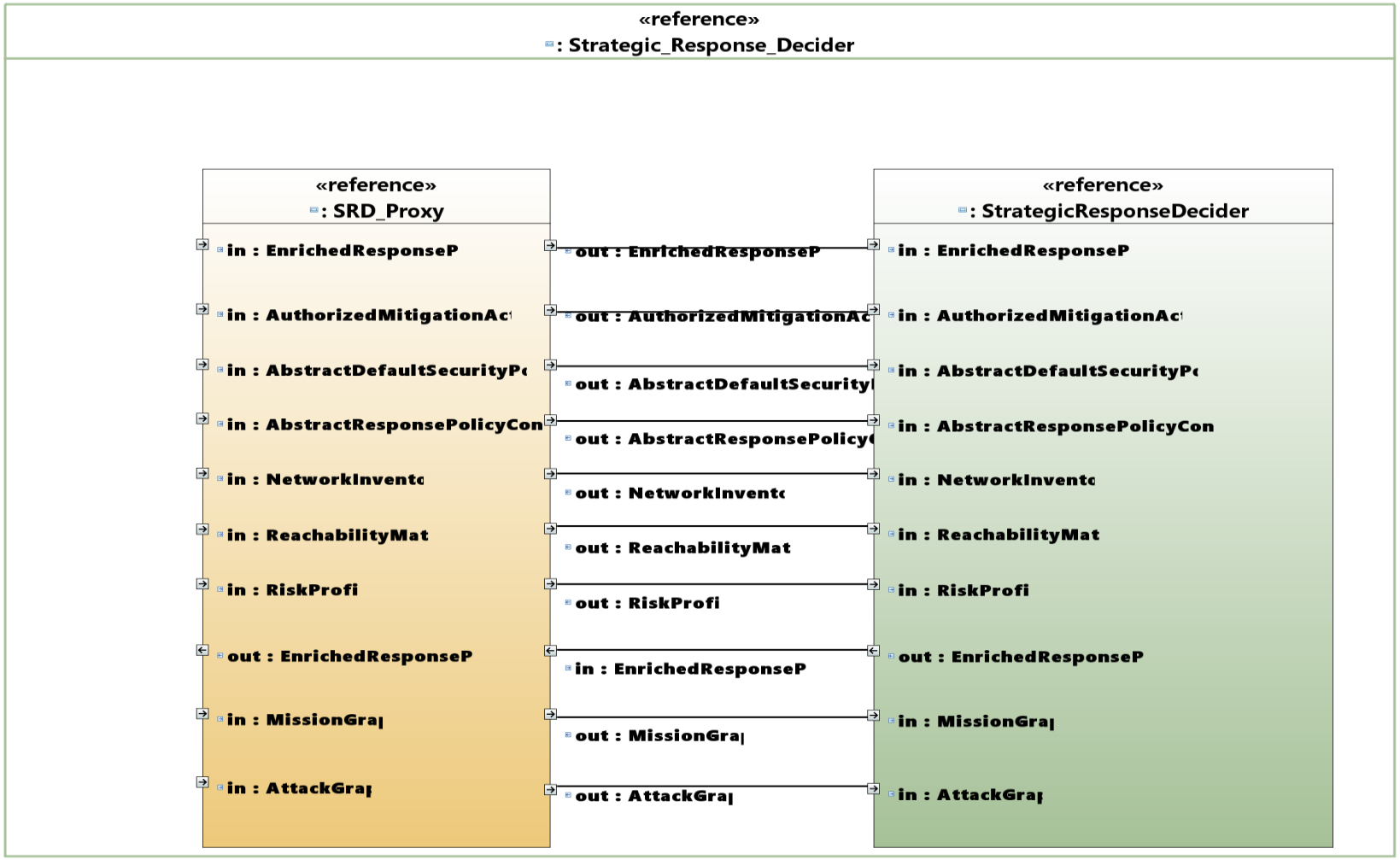


Figure 22 Strategic Response Decider package Logic View

12.3.3 High-Level Online Correlator package Logic View

The High-Level Online Correlator package encompasses these components:

- QueryBasedEngine
- AutomataBasedEngine
- PotentialAttackIdentifier (which have not been developed, since it was optional. It remains in the HLD for sake of completness)

Next Figure depicts a higher level of detail on the HLOC package:

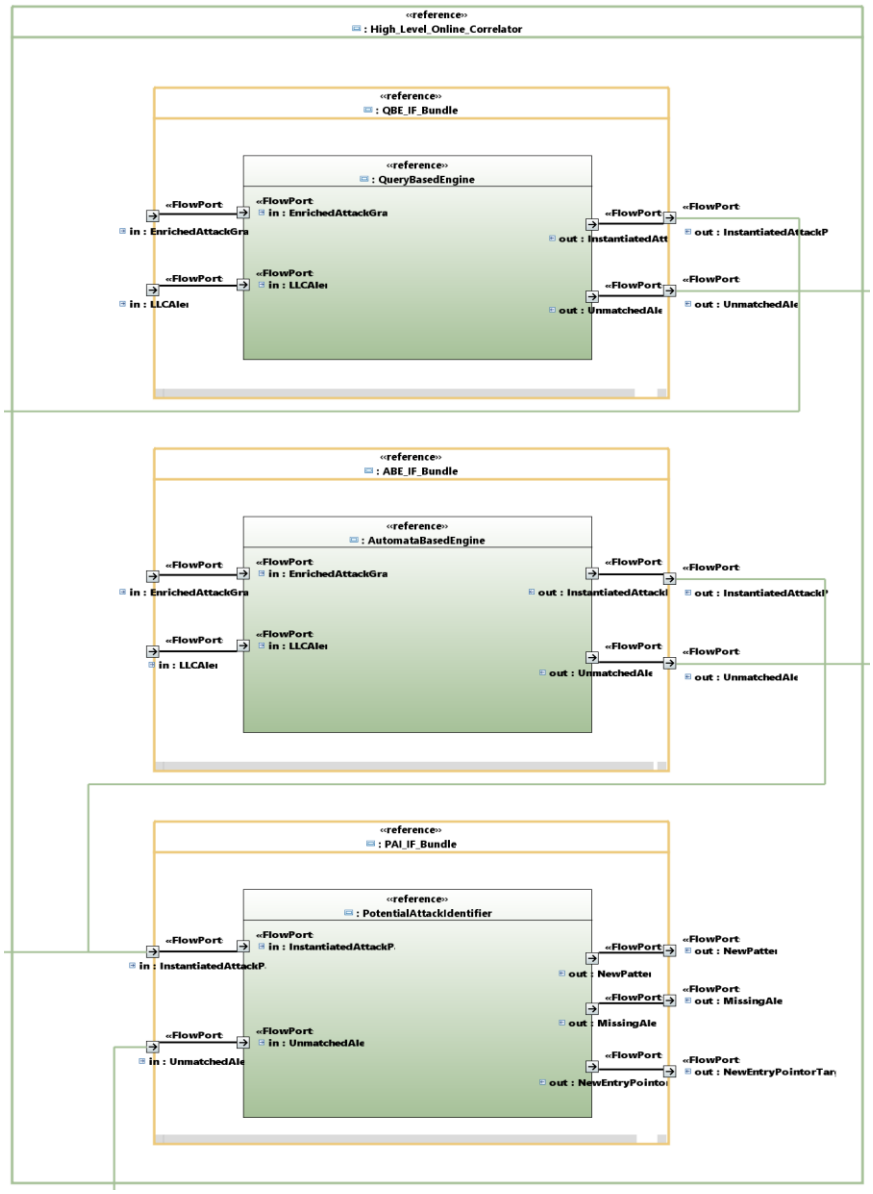


Figure 23 High-Level Online Correlator package Logic View

12.3.4 Tactical Response Decider package Logic View

The Tactical Response Decider package encompasses this component:

- TacticalResponseDecider

Next Figure depicts a higher level of detail on the TRD package:

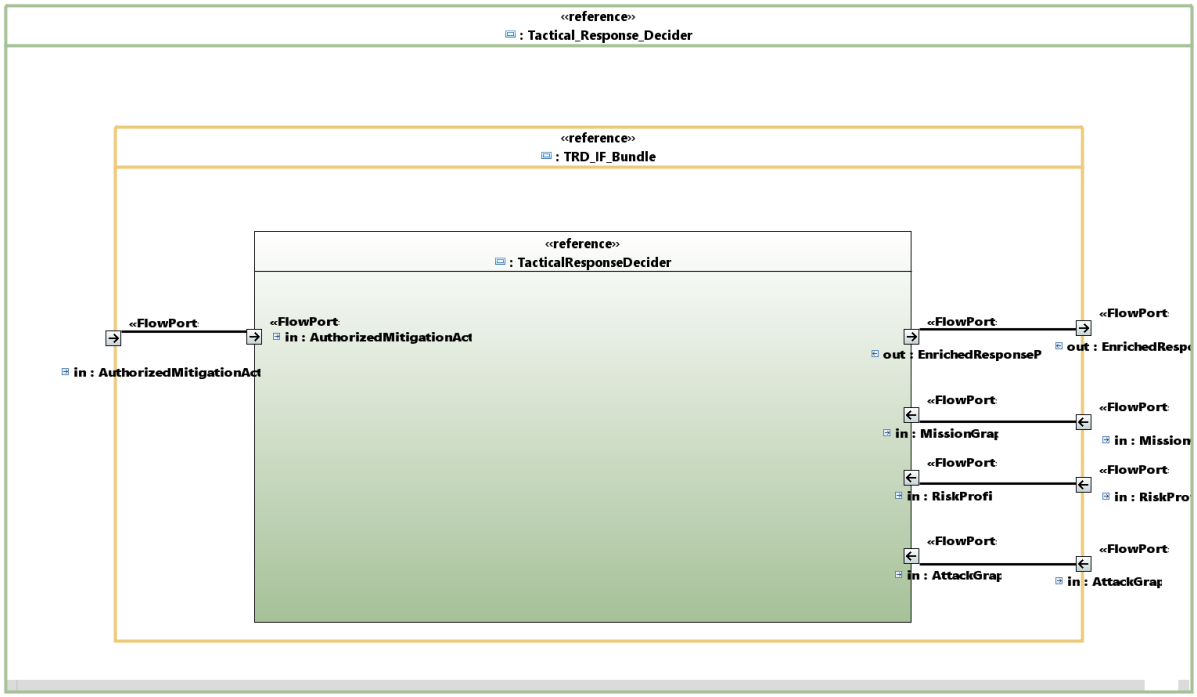


Figure 24 Tactical Response Decider Logic View

12.4 Visualization sub-system

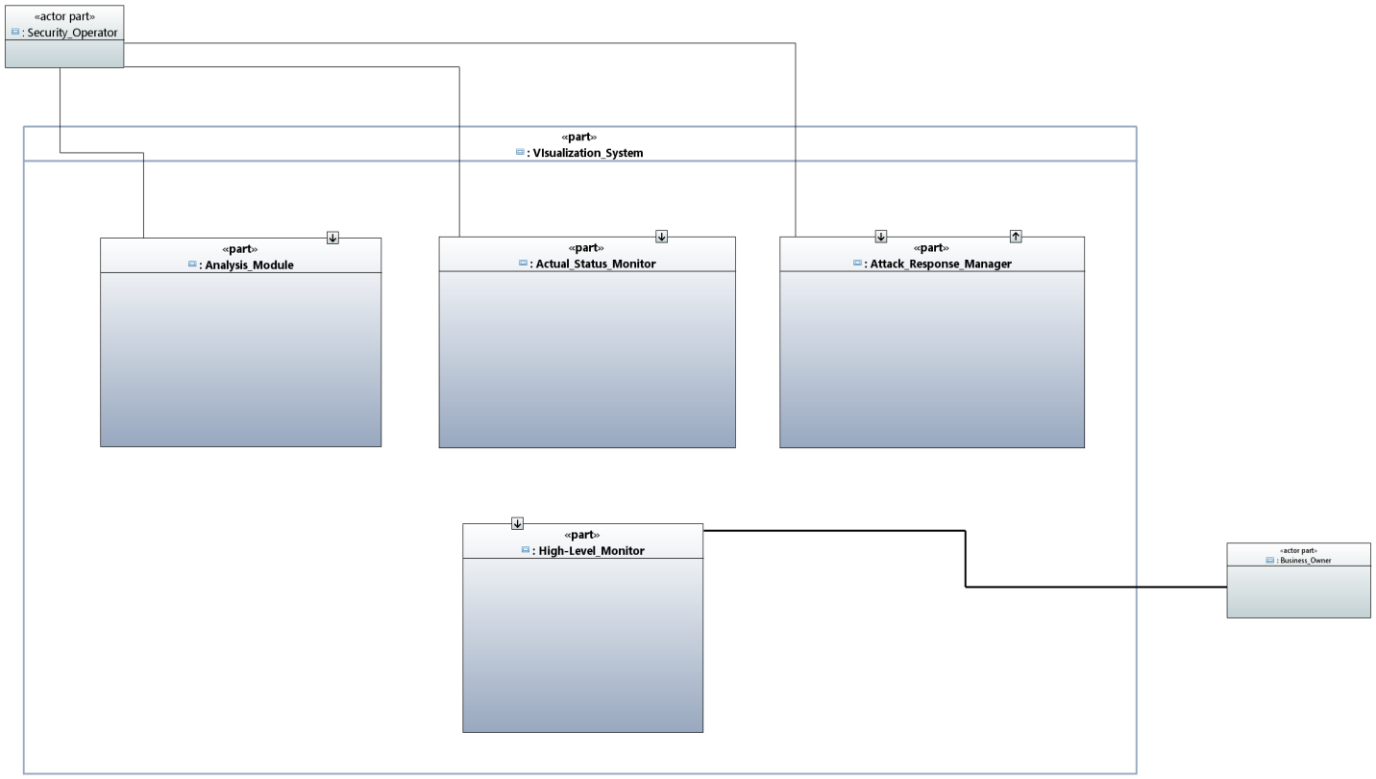


Figure 25 Visualization Sub-System Logic High Level Design overview

12.4.1 Analysis Module/High-Level Monitor Views Logic View

In the actual Design, the High-Level Monitor View is considered as a part of the Analysis Module, with which shares some inputs.

Next Figure depicts a higher level of detail on the Analysis Module/High-Level Monitor Views:

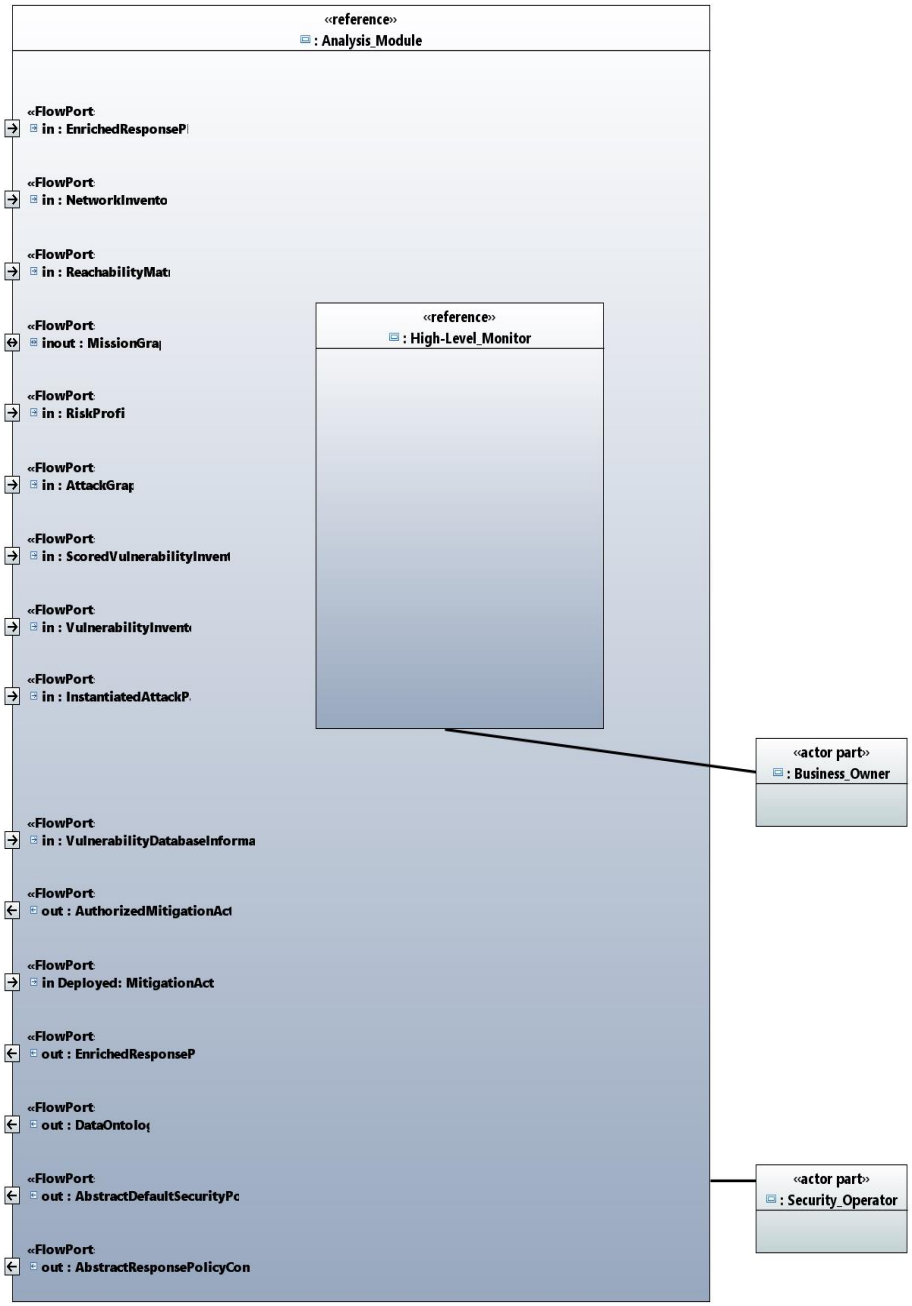


Figure 26 Analysis Module/High-Level Monitor Views Logic View

12.4.2 Actual Status Monitor/Attack Response Manager Views Logic View

In the actual Design, the Attack Response Manager View is considered as a part of the Actual Status Monitor View, with which shares some inputs.

Next Figure depicts a higher level of detail on the Actual Status Monitor/Attack Response Manager Views:

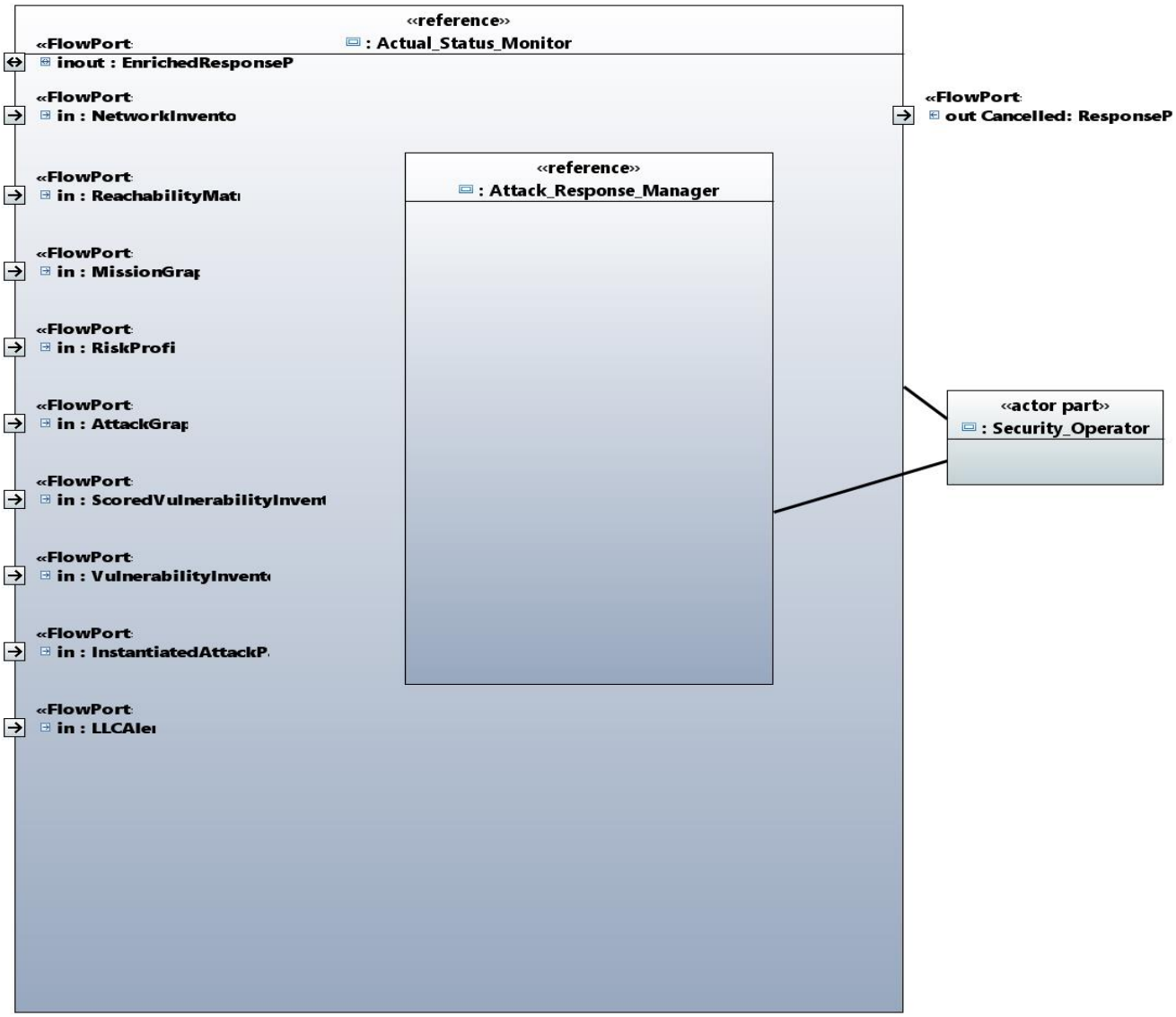


Figure 27 Actual Status Monitor/Attack Response Manager Views Logic View

13 ANNEX B – DETAILED REQUIREMENTS VERIFICATION SUMMARY

In this Annex a summary of the Verification activities over [D4.1.1], [D5.1.1] and [D6.1.1] requirements it is reported.

13.1 Caption

Colour	TC Exists ?	TE Exists?	Deprecated Requirement (will never fulfilled, yet a TC must exist)	Outcome	Redmine Requirement Status
	N	N	N	N	
	Y	N	Y	N	Closed
	Y	N	N	N	In Progress
	Y	Y	N	N (all TEs fail)	Rejected
	Y	Y	N	Partial (not 100% TEs succeeds)	In Progress
	Y	Y	N	Y	Resolved

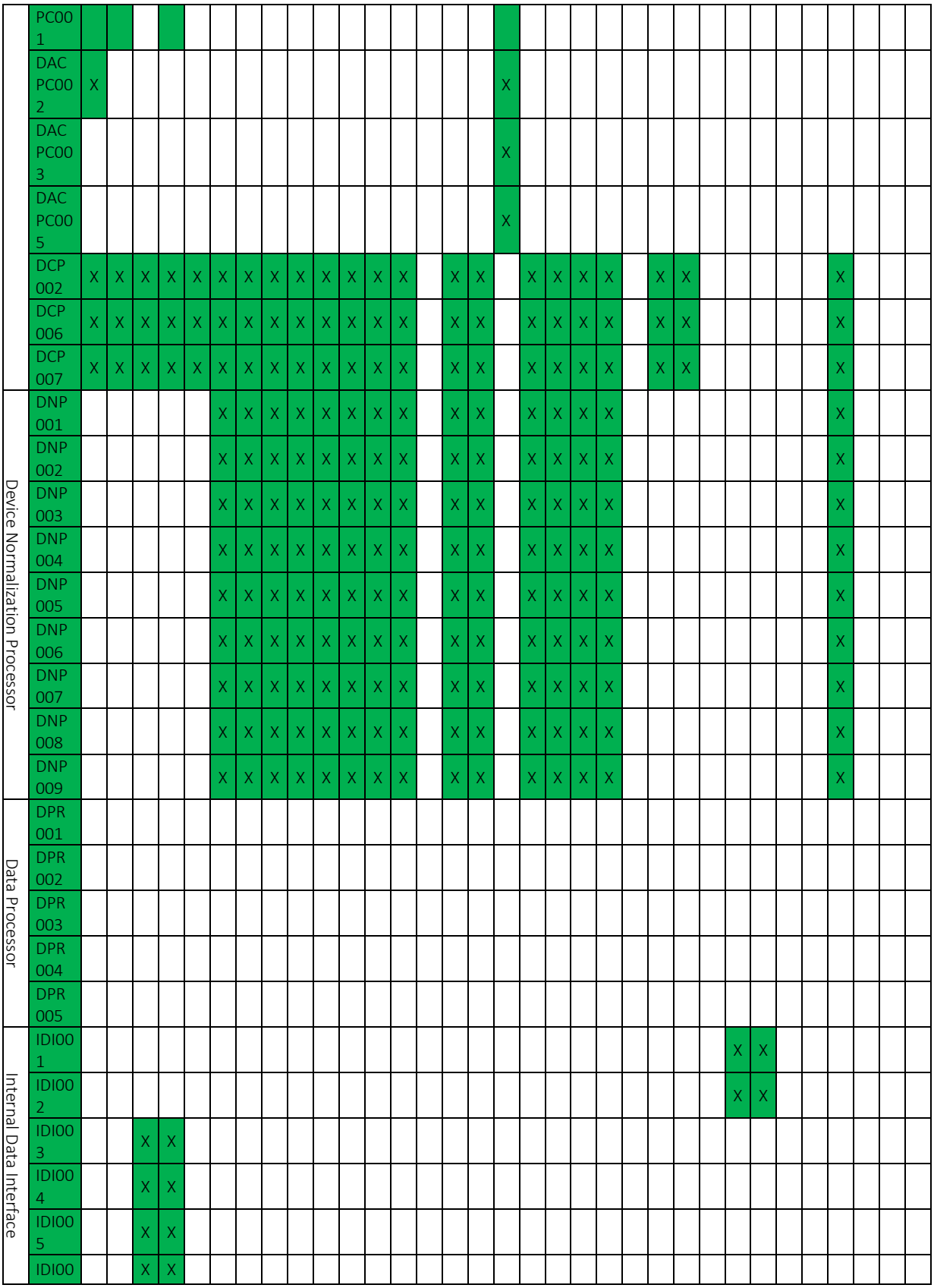
Table 15 - Color Coding used for the final assessment of Requirement coverage

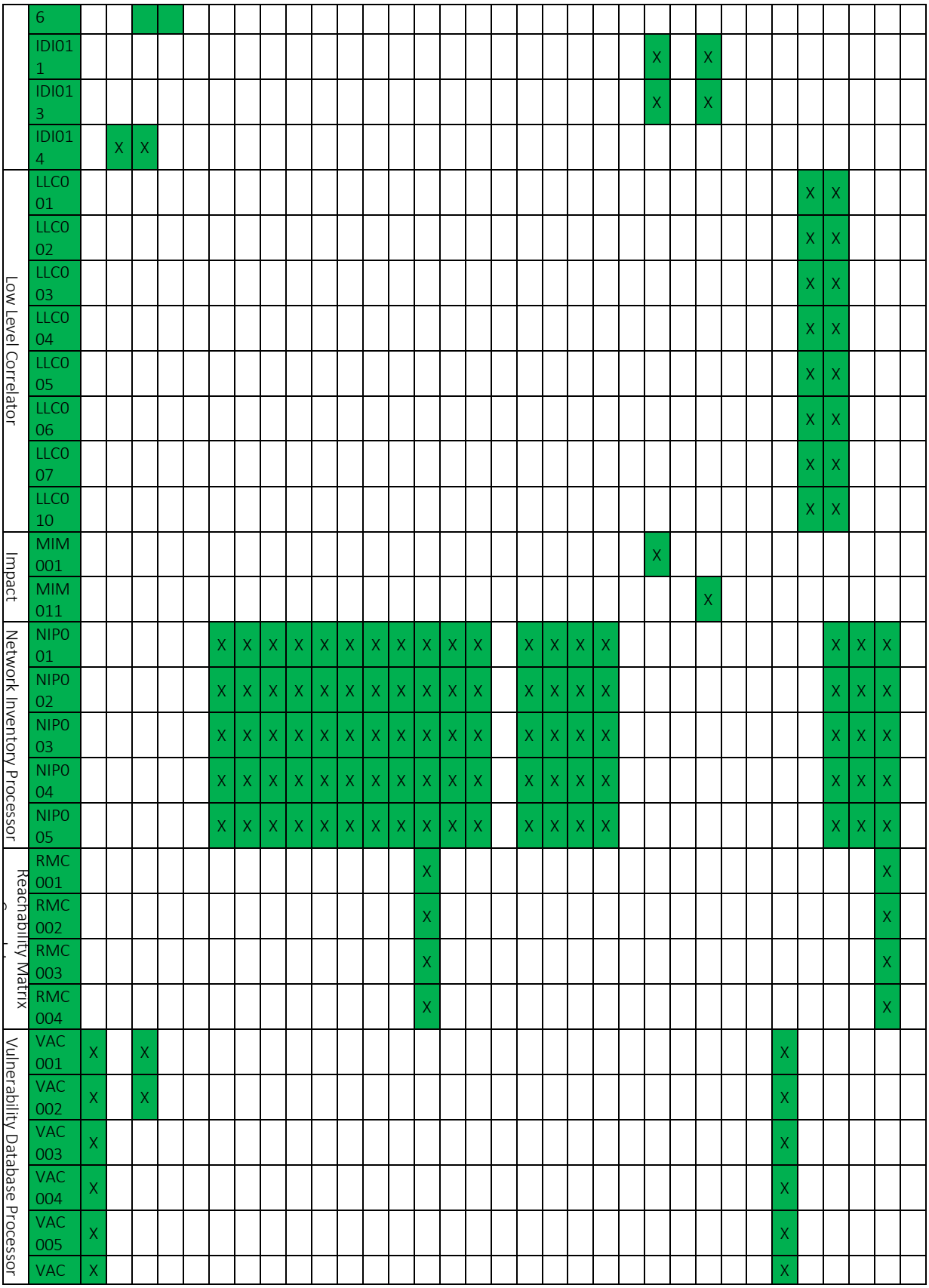
13.2 [D4.1.1] Verification summary

In the next Tables the verification results over [D4.1.1] Requirements are depicted. A more detailed explanation can be found within [D4.3.1R]. The following tables show [D4.1.1] Requirements with respect to the *refine* links with [D2.2.1] Requirements (on the columns).

Table 16 - Verification results summary of [D4.1.1] requirements refining DSC Requirements

		DATA SOURCES AND COLLECTION (DSC) FUNCTIONAL OPERATIONAL REQUIREMENTS																																
		DSC001	DSC002	DSC003	DSC004	DSC005	DSC006	DSC007	DSC008	DSC009	DSC010	DSC011	DSC012	DSC013	DSC014	DSC015	DSC016	DSC017	DSC018	DSC019	DSC020	DSC021	DSC022	DSC023	DSC024	DSC025	DSC026	DSC027	DSC028	DSC029	DSC030	DSC031	DSC032	DSC033
Normalizati	ANP 001																													X	X			
	ANP 002																													X	X			
Business Mission Collector	BMC 001																								X									
	BMC 003																								X									
	BMC 004																								X									
	BMC 005																								X									
	BMC 006																								X									
	BMC 009																								X									
ntr	DAC	X	X		X													X																


Device Normalization Processor
Data Processor
Internal Data Interface
PC001
DAC PC002
DAC PC003
DAC PC005
DCP 002
DCP 006
DCP 007
DNP 001
DNP 002
DNP 003
DNP 004
DNP 005
DNP 006
DNP 007
DNP 008
DNP 009
DPR 001
DPR 002
DPR 003
DPR 004
DPR 005
IDI001
IDI002
IDI003
IDI004
IDI005
IDI00


6
IDI011
IDI013
IDI014
LLC001
LLC002
LLC003
LLC004
LLC005
LLC006
LLC007
LLC010
Low Level Correlator
MIM001
MIM011
Impact
NIP001
NIP002
NIP003
NIP004
NIP005
Network Inventory Processor
RMC001
RMC002
RMC003
RMC004
Reachability Matrix
VAC001
VAC002
VAC003
VAC004
VAC005
VAC
Vulnerability Database Processor

	006																														
	VAC 007	X																									X				
y	VLP001		X																												

Table 17 - Verification results summary of [D4.1.1] requirements refining ICA Requirements

		INFORMATION AND CORRELATION (ICA) FUNCTIONAL OPERATIONAL REQUIREMENTS																
		ICA001	ICA002	ICA003	ICA004	ICA005	ICA006	ICA010	ICA011	ICA012	ICA013	ICA014	ICA015	ICA016	ICA017	ICA018	ICA019	ICA020
Alert Normalization Processor	ANP001	X	X	X	X	X												
	ANP002	X	X	X	X	X												
Device Normalization Processor	DNP001	X	X	X	X	X												
	DNP002	X	X	X	X	X												
	DNP003	X	X	X	X	X												
	DNP004	X	X	X	X	X												
	DNP005	X	X	X	X	X												
	DNP006	X	X	X	X	X												
	DNP007	X	X	X	X	X												
	DNP008	X	X	X	X	X												
	DNP009	X	X	X	X	X												
Data Processor	DPR001	X																
	DPR002	X																
	DPR003	X																
	DPR004	X																
	DPR005	X																
Internal Data Interface	IDI007						X											
	IDI008						X											
Low Level Correlator	LLC001	X																
	LLC002	X																
	LLC003	X																
	LLC004	X																
	LLC005	X																
	LLC006	X																
	LLC007	X																
	LLC010	X																
Mission Impact Module	MIM001																	
	MIM002							X	X	X	X	X	X	X	X	X		
	MIM003							X	X	X	X	X	X	X	X	X		
	MIM004							X	X	X	X	X	X	X	X	X		
	MIM005							X	X	X	X	X	X	X	X	X		

	MIM006							X	X	X	X	X	X	X	X	X		
	MIM008							X	X	X	X	X	X	X	X	X		
	MIM009							X	X	X	X	X	X	X	X	X		
	MIM010							X										
	MIM011							X										
	MIM012							X									X	X
	MIM013							X									X	X
	MIM014							X									X	X
	MIM015							X									X	X
	MIM016							X										
	MIM017							X									X	X
Network Inventory Processor	NIP001	X	X	X	X	X												
	NIP002	X	X	X	X	X												
	NIP003	X	X	X	X	X												
	NIP004	X	X	X	X	X												
	NIP005	X	X	X	X	X												
Persistency Manager	PM001						X											
	PM002						X											
	PM003						X											
	PM004						X											
	PM005						X											
	PM006						X											
	PM007						X											
	PM008						X											
	PM009						X											
	PM010						X											
	PM011						X											
	PM012						X											
	PM013						X											
	PM014						X											
	PM015						X											
	PM016						X											
	PM017						X											
	PM018						X											
	PM019						X											
	PM020						X											
	PM021						X											
	PM022						X											
	PM023						X											
	PM024						X											
	PM025						X											
	PM026						X											
	PM027						X											

	PM028						X											
	PM029						X											
	PM030						X											
	PM031						X											
	PM032						X											
	PM033						X											
	PM034						X											
	PM035						X											
	PM036						X											
	PM037						X											
	PM038						X											
	PM039						X											
	PM040						X											
	PM041						X											
	PM042						X											
	PM043						X											
	PM044						X											
	PM045						X											
	PM046						X											
	PM047						X											
	PM048						X											
	PM049						X											
Vulnerability Processor	VLP001	X	X	X	X	X												
	VLP002	X	X	X	X	X												
	VLP003	X	X	X	X	X												
	VLP004	X	X	X	X	X												
	VLP005	X	X	X	X	X												
	VLP006	X	X	X	X	X												
	VLP007	X	X	X	X	X												
	VLP008	X	X	X	X	X												
	VLP010	X	X	X	X	X												
Vulnerability Normalization Processor	VNP001	X	X	X	X	X												
	VNP002	X	X	X	X	X												
	VNP003	X	X	X	X	X												
	VNP004	X	X	X	X	X												
	VNP005	X	X	X	X	X												
	VNP006	X	X	X	X	X												

Table 18 - Verification results summary of [D4.1.1] requirements refining Non-Functional Requirements (on the rows)

		LLC	MIM	RMC

		LLC008	LLC009	LLC011	MIM018	MIM019	RMC005	RMC006	DCP008	PM050	VLP014	BMC010
Compatibility	CMP001											
	CMP002											
	CMP003											
	CMP004											
	CMP005											
	CMP006											
	CMP007											
	CMP008											
	CMP009											
Maintainability	MNT001											
	MNT002											
	MNT003											
	MNT004											
Performance	PRF001											
	PRF002											
	PRF003											
	PRF004			X								
	PRF005											
	PRF006											
	PRF007											
	PRF008											
Portability	PRT001											
	PRT002											
	PRT003											
	PRT004											
	PRT005											
	PRT006											
Reliability	RLB001											
	RLB002											
	RLB003											
	RLB004	X	X									X
	RLB005											
	RLB006											
	RLB007											
	RLB008											
	RLB009	X	X									
	RLB0010				X	X						
	RLB0011				X	X						
	RLB0012											
	RLB0013											
	RLB0014											

Security	SEC001									X		
	SEC002									X		
	SEC003								X			
	SEC004									X		
	SEC005								X			
	SEC006											
Usability	USG001											
	USG002											
	USG003											

As a conclusion, it is possible to state that [D4.1.1] Verification is completed. All Requirements are verified with the exception of one Importance 2 Requirement from the Non-Functional, which is partially verified. Some Requirements related to the BMC component are not verified, because BMC, as stated within [D4.3.1R] has not been integrated within the PANOPTESEC System. Since the integration was optional, as stated on the Importance 1 Requirements DSC024 from [D2.2.1], these Requirements does not affect the global Verification of [D4.1.1R].

13.3 [D5.1.1] Verification summary

In the next Tables the verification results over [D5.1.1] Requirements are depicted. A more detailed explanation can be found within [D5.4.1R]. The following tables show [D5.1.1] Requirements with respect to the *refine* links with [D2.2.1] Requirements (on the columns).

Table 19 - Verification results summary of [D5.1.1] requirements refining PRS Requirements

		Proactive Response System (PRS) Functional Operational Requirements																	
		PRS01	PRS02	PRS03	PRS04	PRS05	PRS06	PRS07	PRS08	PRS09	PRS10	PRS11	PRS12	PRS13	PRS14	PRS15	PRS16	PRS17	PRS22
Gener	WP5.GEN.R1	X	X	X	X	X	X	X	X	X									
	WP5.GEN.R2	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X		X	
	WP5.GEN.R3										X	X	X	X	X	X		X	
Attack Graph Generation	WP5.AGG.R1	X	X	X					X	X				X					
	WP5.AGG.R2	X	X	X	X	X				X				X					
	WP5.AGG.R3	X	X	X			X		X	X				X					
	WP5.AGG.R4	X	X	X					X	X				X					
	WP5.AGG.R5	X	X	X					X	X				X					
	WP5.AGG.R6	X	X	X					X	X				X					
	WP5.AGG.R7	X	X	X	X	X				X				X					
	WP5.AGG.R8	X	X	X					X	X				X					
	WP5.AGG.R9	X	X	X			X		X	X				X					
	WP5.AGG.R10	X	X	X					X					X					
	WP5.AGG.R15	X	X	X				X			X	X		X					
High-level Online correlation	WP5.HOC.R1																		
	WP5. HOC.R2																		
	WP5. HOC.R3																		
	WP5. HOC.R4																		
	WP5. HOC.R5																		
	WP5. HOC.R6																		

	WP5. HOC.R7																		
	WP5. HOC.R8																		
	WP5. HOC.R9																		
	WP5. HOC.R12																		
Potential	WP5.PAI.R1																		
	WP5.PAI.R2																		
	WP5.PAI.R3																		
	WP5.PAI.R4																		
Risk quantification	WP5.RQU. R1	X						X	X	X	X	X						X	
	WP5.RQU. R2	X																	
	WP5.RQU. R3	X						X	X	X	X	X						X	
	WP5.RQU. R4																		
	WP5.RQU. R5	X						X	X	X	X	X						X	
	WP5.RQU. R6	X						X	X	X	X	X						X	
	WP5.RQU. R8	X						X	X	X	X	X						X	
	WP5.RQU. R9																		
	WP5.RQU. R10	X						X	X	X	X	X						X	
	WP5.RQU. R11	X						X	X	X	X	X						X	
	WP5.RQU. R12																		
	WP5.RQU. R13	X						X	X	X	X	X						X	
	WP5.RQU. R14																		
	WP5.RQU. R15	X						X	X	X	X	X						X	
	WP5.RQU. R16	X						X	X	X	X	X						X	
	WP5.RQU. R17	X									X	X						X	
	WP5.RQU. R18	X									X	X						X	
	WP5.RQU. R21	X						X	X	X	X	X						X	
L	WP5.LA.R1	X						X		X	X							X	

	WP5.LA.R2	X						X		X	X							X	
	WP5.LA.R3	X						X		X	X							X	
	WP5.LA.R4																		
	WP5.LA.R5																		
	WP5.LA.R6	X						X		X	X							X	
	WP5.LA.R7																		
	WP5.LA.R8	X						X		X	X							X	
	WP5.LA.R9	X						X		X	X							X	
	WP5.LA.R10																		
	WP5.LA.R11																		
	WP5.LA.R12	X									X							X	
	WP5.LA.R13	X									X							X	
Impact Assessment Functional Requirements	WP5.TIA.R1	X						X	X	X	X	X							
	WP5.TIA.R2	X						X	X	X	X	X							
	WP5.TIA.R3																		
	WP5.TIA.R4	X						X	X	X	X	X							
	WP5.TIA.R5	X						X	X	X	X	X							
	WP5.TIA.R6	X									X	X							
	WP5.TIA.R7	X									X	X							
	WP5.TIA.R9	X						X	X	X	X	X							
	WP5.ROI.R1								X			X							
	WP5.ROI.R2								X			X							
	WP5.ROI.R3								X			X							
	WP5.ROI.R4								X			X							
	WP5.ROI.R5																		
	WP5.RFI.R1	X																X	
	WP5.RFI.R2	X																X	
	WP5.RFI.R3	X																X	
	WP5.RFI.R4	X																X	

	WP5.RFI.R5	X																X	
Strategic Response Decision	WP5.SRD.R 1	X									X	X	X		X	X		X	
	WP5.SRD.R 2	X									X	X	X		X	X		X	
	WP5.SRD.R 3	X									X	X	X		X	X		X	
	WP5.SRD.R 4	X									X	X	X		X	X		X	
	WP5.SRD.R 5	X									X	X			X	X		X	
Security Policy Instantiation	WP5.SPI.R1																X	X	X
	WP5. SPI.R2																X	X	X
	WP5. SPI.R3																X	X	X
	WP5. SPI.R4																X	X	X
	WP5. SPI.R5																X	X	X
	WP5. SPI.R7																X	X	X
Tactical Response Decision	WP5.TRD.R 1																		
	WP5.TRD.R 2																		
	WP5.TRD.R 5																		
	WP5.TRD.R 6																		
	WP5.TRD.R 7																		

Table 20 – Verification results summary of [D5.1.1] requirements refining RRS Requirements

		Reactive Response System (RRS) Functional Operational Requirements																						
		RRS01	RRS02	RRS03	RRS04	RRS05	RRS06	RRS07	RRS08	RRS09	RRS10	RRS11	RRS12	RRS13	RRS14	RRS15	RRS16	RRS17	RRS18	RRS23	RRS24	RRS25	RRS26	RRS27
General	WP5.GEN.R1	X	X	X	X	X	X	X	X	X														
	WP5.GEN.R2	X	X	X	X	X	X	X	X	X	X	X	X	X			X		X	X				
	WP5.GEN.R3										X	X	X	X			X		X					
Attack Graph Generation	WP5.AGG.R1	X	X					X	X								X						X	
	WP5.AGG.R2	X	X		X	X		X									X						X	
	WP5.AGG.R3	X	X				X	X									X						X	
	WP5.AGG.R4	X	X					X	X								X						X	
	WP5.AGG.R5	X	X					X	X								X						X	
	WP5.AGG.R6	X	X					X	X								X						X	
	WP5.AGG.R7	X	X		X	X		X									X						X	
	WP5.AGG.R8	X	X					X									X						X	
	WP5.AGG.R9	X	X				X	X									X						X	
	WP5.AGG.R10	X	X					X									X						X	
	WP5.AGG.R15	X	X					X	X	X	X		X				X					X	X	
High-level Online correlation	WP5.HOC.R1	X	X	X				X																
	WP5. HOC.R2	X	X	X				X																
	WP5. HOC.R3	X	X	X																X				X
	WP5. HOC.R4	X	X	X	X		X										X					X		
	WP5. HOC.R5	X	X	X																				
	WP5. HOC.R6	X	X	X																				
	WP5. HOC.R7	X	X	X	X		X											X					X	

	WP5.HOC.R8	X	X	X	X											X	X				X	X		
	WP5.HOC.R9	X	X	X																				X
	WP5.HOC.R12	X	X	X	X																			X
Potential Attack	WP5.PAI.R1	X																	X					
	WP5.PAI.R2	X																	X					
	WP5.PAI.R3	X																	X					
	WP5.PAI.R4	X																	X					
Risk quantification	WP5.RQU.R1	X	X					X	X	X	X		X						X					
	WP5.RQU.R2	X	X	X	X	X	X	X		X	X		X						X					
	WP5.RQU.R3																							
	WP5.RQU.R4	X	X	X	X	X	X	X	X	X	X		X						X					
	WP5.RQU.R5	X	X	X	X	X	X	X	X	X	X		X						X					
	WP5.RQU.R6	X	X	X	X	X	X	X	X	X	X		X						X					
	WP5.RQU.R8																							
	WP5.RQU.R9	X	X	X	X	X	X	X	X	X	X		X						X					
	WP5.RQU.R10	X	X	X	X	X	X	X	X	X	X		X						X					
	WP5.RQU.R11	X	X							X	X		X						X					
	WP5.RQU.R12	X	X	X	X	X				X	X		X						X					
	WP5.RQU.R13																							
	WP5.RQU.R14	X	X	X	X	X	X	X	X	X	X		X						X					
	WP5.RQU.R15	X	X	X	X	X	X	X	X	X	X		X						X					
	WP5.RQU.R1	X	X	X	X	X	X	X	X	X	X		X						X					

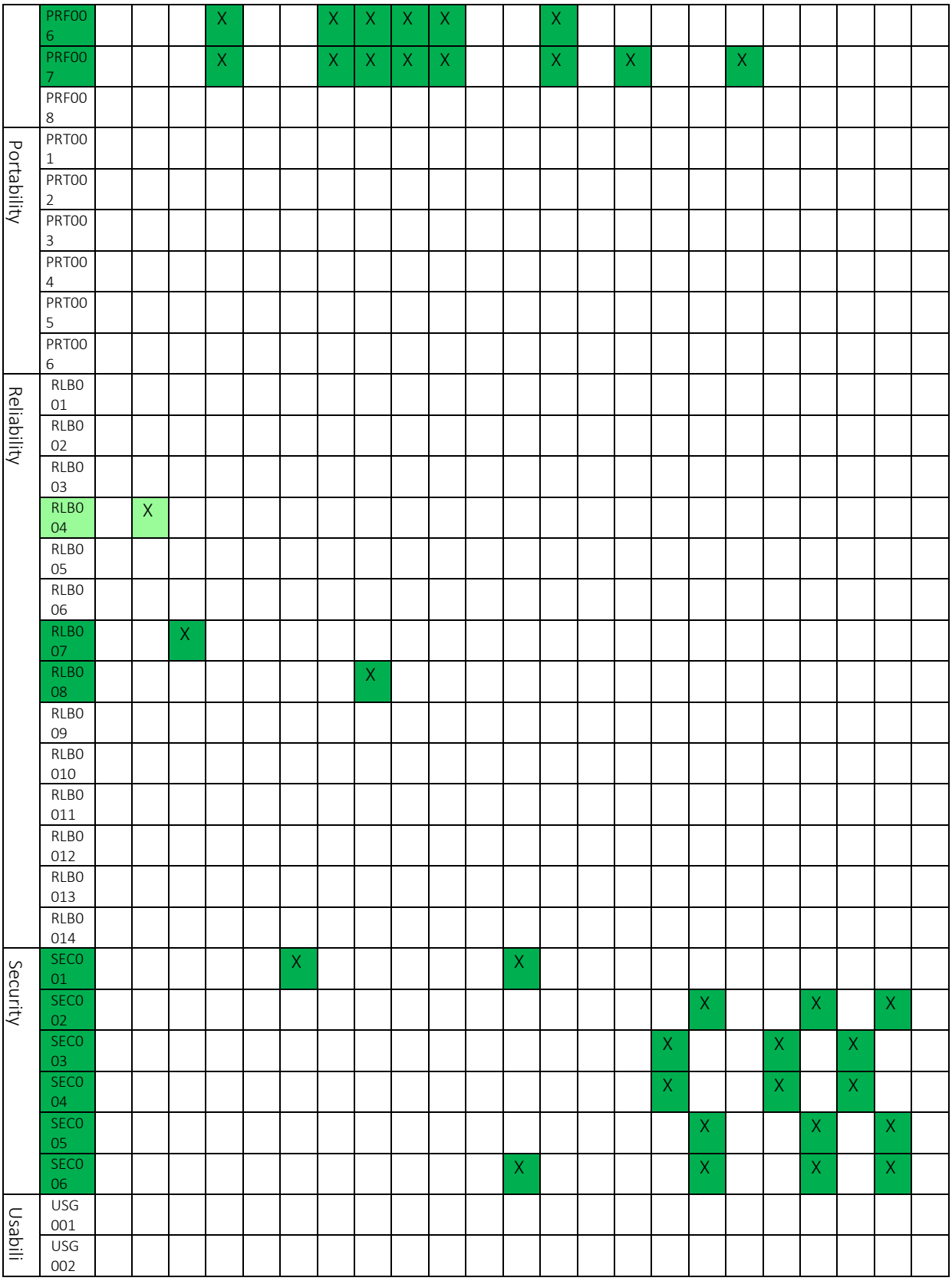
	6																						
	WP5.RQU.R17	X	X	X	X	X	X	X		X	X		X						X					
	WP5.RQU.R18	X	X	X	X	X	X	X		X	X		X						X					
	WP5.RQU.R21	X	X						X	X	X		X						X					
Likelihood Assessment	WP5.LA.R1																							
	WP5.LA.R2	X	X	X	X	X	X	X		X			X						X					
	WP5.LA.R3																							
	WP5.LA.R4	X	X	X	X	X	X	X		X			X						X					
	WP5.LA.R5	X	X	X	X	X	X	X		X			X						X					
	WP5.LA.R6																							
	WP5.LA.R7	X	X	X	X	X	X	X		X			X						X					
	WP5.LA.R8	X	X	X	X	X	X	X		X			X						X					
	WP5.LA.R9																							
	WP5.LA.R10	X	X	X	X	X	X	X		X			X						X					
	WP5.LA.R11	X	X	X	X	X	X	X		X			X						X					
	WP5.LA.R12	X	X	X	X	X	X	X		X			X						X					
	WP5.LA.R13	X	X	X	X	X	X	X		X			X						X					
Impact Assessment Functional	WP5.TIA.R1	X	X						X	X	X	X												
	WP5.TIA.R2																							
	WP5.TIA.R3	X	X						X	X	X	X												
	WP5.TIA.R4	X	X						X	X	X	X												
	WP5.TIA.R5	X	X						X	X	X	X												
	WP5.TIA.R6	X	X								X	X												
	WP5.TIA.R7	X	X								X	X												

	WP5.TIA.R9	X	X						X	X	X	X												
	WP5.ROI.R1								X		X													
	WP5.ROI.R2								X		X													
	WP5.ROI.R3								X		X													
	WP5.ROI.R4								X		X													
	WP5.ROI.R5																							
	WP5.RFI.R1																							
	WP5.RFI.R2																							
	WP5.RFI.R3																							
	WP5.RFI.R4																							
	WP5.RFI.R5																							
Strategic Response Decision	WP5.SRD.R1																							
	WP5.SRD.R2																							
	WP5.SRD.R3																							
	WP5.SRD.R4																							
	WP5.SRD.R5																							
Security Policy Instantiation	WP5.SPI.R1																		X					
	WP5.SPI.R2																		X					
	WP5.SPI.R3																		X					
	WP5.SPI.R4																		X					
	WP5.SPI.R5																		X					
	WP5.SPI.R7																		X					
Tactical	WP5.TRD.R1	X	X							X		X	X											
	WP5.TRD.R2	X								X			X											
	WP5.TRD.R5	X	X							X			X											

	WP5.TRD.R6	X	X							X			X										
	WP5.TRD.R7												X	X	X								

Table 21 – Verification results summary of [D5.1.1] requirements refining Non-Functional Requirements (on the rows)

		GEN				AGG	HOC				PAI		RQU	ROI		RFI			SRD			SPI		
		WP5.GEN.R7	WP5.GEN.R6	WP5.GEN.R5	WP5.GEN.R4	WP5.AGG.R18	WP5.HOC.R16	WP5.HOC.R15	WP5.HOC.R14	WP5.HOC.R13	WP5.PAI.R6	WP5.PAI.R5	WP5.RQU.R19	WP5.ROI.R7	WP5.ROI.R6	WP5.RFI.R6	WP5.RFI.R7	WP5.RFI.R8	WP5.SRD.R6	WP5.SRD.R7	WP5.SRD.R8	WP5.SPI.R8	WP5.SPI.R9	WP5.TRD.R8
Compatibility	CMP001																							
	CMP002																							
	CMP003																							
	CMP004																							
	CMP005	X																						
	CMP006	X																						
	CMP007																							
	CMP008																							
	CMP009	X																						
Maintainability	MNT001																							
	MNT002																							
	MNT003																							
	MNT004																							
Performance	PRF001				X									X		X			X					
	PRF002																							
	PRF003																							
	PRF004				X	X									X	X								X
	PRF005																							


PRF006
PRF007
PRF008
Portability
PRT001
PRT002
PRT003
PRT004
PRT005
PRT006
Reliability
RLB001
RLB002
RLB003
RLB004
RLB005
RLB006
RLB007
RLB008
RLB009
RLB010
RLB011
RLB012
RLB013
RLB014
Security
SEC001
SEC002
SEC003
SEC004
SEC005
SEC006
Usabili
USG001
USG002

	USG 003																													

As a conclusion, it is possible to state that [D5.1.1] Verification is completed. All Requirements are verified with the exception of one Importance 2 Requirement from the Non-Functional group, which is partially verified, plus the Requirements related to the PAI component, which is optional, as stated in WP5.PAI.R6.

13.4 [D6.1.1] Verification Summary

In the next Tables the verification results over [D6.1.1] Requirements are depicted. A more detailed explanation can be found within [D6.3.1R]. The following tables show [D6.1.1] Requirements with respect to the *refine* links with [D2.2.1] Requirements (on the columns).

Table 22 - Verification results summary of [D6.1.1] requirements refining VIZ Requirements

		VIZ001	VIZ002	VIZ003	VIZ004	VIZ005	VIZ006	VIZ007	VIZ008	VIZ009	VIZ010	VIZ011	VIZ012	VIZ013	VIZ014	VIZ015	VIZ016	VIZ017	VIZ018	VIZ019	VIZ020	VIZ021	VIZ022	VIZ023	VIZ024	VIZ025	VIZ026	VIZ027	VIZ028	VIZ029	VIZ030
WP6.Gen.R1	multiple syncronized views	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
	WP6.Gen.R1.SR1	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
	WP6.Gen.R1.SR2	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
	WP6.Gen.R1.SR3	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
	WP6.Gen.R1.SR4	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
	WP6.Gen.R1.SR5	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
	WP6.Gen.R1.SR6	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
	WP6.Gen.R1.SR7	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
	WP6.Gen.R1.SR8	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
	WP6.Gen.R1.SR9	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
WP6.Gen.	collaboration	x																											x		

R2																														
	WP6.Gen.R2.SR1	x																										x		
	WP6.Gen.R2.SR2	x																										x		
	WP6.Gen.R2.SR3	x																										x		
	WP6.Gen.R2.SR4	x																										x		
	WP6.Gen.R2.SR5	x																										x		
WP6.Gen.R3	Time machine																						x	x	x					
	WP6.Gen.R3.SR1																						x	x	x					
	WP6.Gen.R3.SR2																						x	x	x					
WP6.ANM.R1	graph level 3 ->GEO								x																				x	
	WP6.ANM.R1.SR1																													
	WP6.ANM.R1.SR2																													
WP6.ANM.R2	mission graph	x													x	x		x	x	x										
	WP6.ANM.R2.SR1	x													x	x		x												
	WP6.ANM.R2.SR2														x	x			x											
	WP6.ANM.R2.SR3														x	x				x										
WP6.ANM.R3	vulnerabilities									x												x	x							
	WP6.ANM.R3.SR1								x	x												x	x							
	WP6.ANM.R3.									x												x	x							

	SR2																													
	WP6.ANM.R3.SR3									x													x	x						
WP6.ANM.R4	attack paths										x																			
WP6.ANM.R5	mitigation actions												x	x			x													
	WP6.ANM.R5.SR1												x																	
	WP6.ANM.R5.SR2												x																	
	WP6.ANM.R5.SR3	x											x																	
	WP6.ANM.R5.SR4												x																	
	WP6.ANM.R5.SR5													x			x													
	WP6.ANM.R5.SR6													x																
WP6.ANM.R6	hystory	x																						x						
	WP6.ANM.R6.SR1																							x	x	x				
	WP6.ANM.R6.SR2																							x	x	x				
WP6.ANM.R7	configure							x																						
	WP6.ANM.R7.SR1							x																						
	WP6.ANM.R7.SR2																	x												
	WP6.ANM.R7.SR3																	x												
WP6.ANM.R8	risk & mission impact		x	x			x																							

	WP6.ANM.R8.SR1		x	x			x																								
	WP6.ANM.R8.SR2		x	x			x																								
	WP6.ANM.R8.SR3		x	x			x																								
WP6.MON.R1	graph level 3 ->GEO	x			x				x																				x		
	WP6.MON.R1.SR1	x																													
	WP6.MON.R1.SR2	x																													
	WP6.MON.R1.SR4	x			x																										
	WP6.MON.R1.SR5	x																													
WP6.MON.R2	inst attack path -> dynamic risk	x																													
	WP6.MON.R2.SR1	x																													
	WP6.MON.R2.SR2	x																													
	WP6.MON.R2.SR3	x																													
	WP6.MON.R2.SR4	x																													
	WP6.MON.R2.SR5	x																													
WP6.MON.R3	dynamic mission impact	x				x																						x			
	WP6.MON.R3.SR1	x				x																									
	WP6.MON.R3.SR2	x				x																						x			
WP6.MON.R4	dynamic risk level	x			x																							x			

	WP6.MON.R4.SR1	x			x																										
	WP6.MON.R4.SR2	x			x																										
	WP6.MON.R4.SR3	x			x																										
WP6.MON.R5	alerts	x										x								x											
	WP6.MON.R5.SR1	x										x								x											
	WP6.MON.R5.SR2	x										x								x											
WP6.ARM.R1	dyn risk & anticipated Mimpact	x			x	x																						x			
	WP6.ARM.R1.SR1	x			x	x																						x			
	WP6.ARM.R1.SR2	x			x	x																						x			
WP6.ARM.R2	response plan	x													x	x															
	WP6.ARM.R2.SR1	x													x	x															
	WP6.ARM.R2.SR2	x													x	x															
	WP6.ARM.R2.SR3	x													x	x															
WP6.ARM.R3	stop																										x				
WP6.HLM.R1	Executive monitoring	x	x	x	x	x																									
	WP6.HLM.R1.SR1	x	x	x	x	x																									
	WP6.HLM.R1.SR2	x	x	x	x	x																									
	WP6.HL	x	x	x	x	x																									

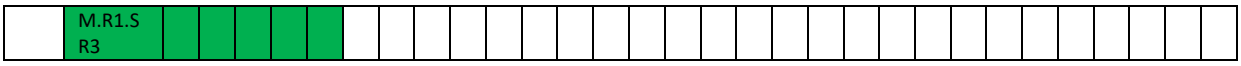

M.R1.S
R3

Table 23 - Verification results summary of [D6.1.1] requirements refining Non-Functional Requirements (on the rows)

		WP6.PRF.R1	WP6.PRF.R2	WP6.CMP.R1	WP6.CMP.R2	WP6.CMP.R3	WP6.CMP.R4	WP6.USG.R1	WP6.USG.R2	WP6.USG.R3	WP6.RLB.R01	WP6.RLB.R02	WP6.SEC.R01	WP6.SEC.R02	WP6.MNT.R01	WP6.MNT.R02	WP6.PRT.R01	WP6.PRT.R02
Compatibility	CMP001																	
	CMP002																	
	CMP003																	
	CMP004																	
	CMP005																	
	CMP006																	
	CMP007																	
	CMP008																	
	CMP009						x											
Maintainability	MNT001															x		
	MNT002																	
	MNT003																	
	MNT004																	
Performance	PRF001																	
	PRF002																	
	PRF003																	
	PRF004		x															
	PRF005																	
	PRF006																	
	PRF007																	
	PRF008																	
Portability	PRT001																	x
	PRT002																	
	PRT003																	
	PRT004																	
	PRT005																	
	PRT006																	
Reliability	RLB001										x							
	RLB002										x							
	RLB003										x							
	RLB004																	
	RLB005																	
	RLB006																	
	RLB007																	
	RLB008											x						

	RLB009																	
	RLB0010																	
	RLB0011																	
	RLB0012																	
	RLB0013																	
	RLB0014																	
Security	SEC001																	
	SEC002																	
	SEC003													x				
	SEC004												x					
	SEC005																	
	SEC006																	
Usability	USG001							x										
	USG002																	
	USG003									x								

As a conclusion, it is possible to state that [D6.1.1] Verification is completed. All Requirements are verified, with the exception of some Importance 2 Requirements, which will not be developed.