FP7-610416-PANOPTESEC

Dynamic Risk Approaches for Automated Cyber Defence

D8.1.2 – Dissemination and Exploitation Plan

Work-Package	WP8	Deliverable	D8.1.2
Due Date	M36	Submission Date	22-11-2016
Main Author(s)	RHEA, ACEA		
Contributors	All project participants		
Version	V3.1	Status	Final
Dissemination Level	CO	Nature	R
Keywords	Dissemination, publicity, website, social media, events, publications, external communications, commercialisation		

Part of the Seventh

Framework Programme

Funded by the EC - DG Connect

EXECUTIVE SUMMARY

This is the deliverable D8.1.2 - Dissemination and Exploitation Plan of the FP7 project Dynamic Risk Approaches for Automated Cyber Defence (PANOPTESEC). This work was carried out as part of the WP8 Dissemination and Demonstration and specifically Task 8.1 Information Dissemination.

An important goal of the PANOPTESEC project is to ensure the sustainability of the project's outcomes through the Dissemination & Exploitation activities to be developed during the project and will continue after its completion. This plan sets the direction of future actions and summarises the roadmap for exploitation of the results.

In this report, the outline of the Dissemination and Exploitation (D&E) activities are presented, including the implementation of the project website, implementation of social media channels along with a description of dissemination and exploitation targets. Moreover, a list of other Dissemination activities, including publications, presentations, press releases, articles and conference participation is presented as well as a summary of collaborations and synergies with other projects. Finally, the methodology followed in the development of the Exploitation Plans for PANOPTESEC and how each partner plans to exploit the results of the project is described.

It is not intended that this document provide extensive details of dissemination and exploitation activities or results since these results are otherwise presented in the D8.1.3 Dissemination and D8.1.4 Exploitation Reports.

HISTORY

Version	Date	Name/Partner	Comment
V1	30-04-2014	Paulina Reizi/RHEA	Initial creation of the document.
V1.1	12-03-2015	Hervé Debar/IMT	Input from IMT about the exploitation plan
V1.2	23-03-2015	Paulina Reizi/RHEA	Updated document with latest publications and conferences, project workshops planning, collaboration with organisations and other projects, placeholder for individual partner exploitation plans and other required updates based on the EC review and project progress
V1.2.1	24-03-2015	Doug Wiemer/RHEA	Input from RHEA about the exploitation plan
V1.2.2	25-03-2015	Ralf Möller/UzL	Input from UzL about the exploitation plan
V1.2.3	25-03-2015	Samuel Dubus/ALBFL	Input from ALBLF about the exploitation plan
V1.3	25-03-2015	Paulina Reizi/RHEA	Submitted draft version for preliminary QA review
V1.3.1	26-03-2015	Nicolas Prigent/ Supélec	Input from CentraleSupélec about the exploitation plan
V1.3.2	26-03-2015	Silvia Bonomi/CIS-UROME	Input from CIS-UROME about the exploitation plan
V1.3.3	26-03-2015	Samuel Dubus/ALBLF	Additional input from ALBLF about the exploitation plan
V1.3.4	26-03-2015	Andrea Guarino/ACEA	Input from ACEA about the exploitation plan
V1.3.5	26-03-2015	Horacio Brizuela/ Epistematica	Input from Epistematica about the exploitation plan
V1.4	26-03-2015	Paulina Reizi/RHEA	Integrated all inputs and submitted revised version for final QA review
V1.5	26-03-2015	Giuseppe Santucci/CIS-UROME	QA review and final comments
V2.0	27-03-2015	Paulina Reizi/RHEA	Added graphic representation of the website visitors' behaviour and implemented few changes based on the QA review. Submitted revised document.
V2.1	27-5-2015	Paulina Reizi/RHEA	Insert history details, updated the Roadmap and added the latest dissemination activities
V2.2	03-06-2015	Doug Wiemer/RHEA	Additional input from RHEA about the exploitation plan
V2.3	03-06-	Samuel	Additional input from ALBFL about the

	2015	Dubus/ALBFL	exploitation plan
V2.4	03-06-2015	Luca Severini/ Epistematica	Additional input from Epistematica about the exploitation plan
V2.5	03-06-2015	Paulina Reizi/RHEA	Integrated all inputs and submitted revised version for QA review
V2.6	05-06-2015	Palmer Colamarino/RHEA	QA review
V2.7	05-06-2015	Paulina Reizi/RHEA	Updates following QA review
V3.0	05-06-2015	Douglas Wiemer/RHEA	Draft V2.7 approved by QA. Published as V3.0 Final.
V3.1	22-11/2016	Douglas Wiemer/RHEA	Updated for completeness and consistency to D8.1.3 Dissemination and D8.1.4 Exploitation reports.

TABLE OF CONTENTS

TABLE OF FIGURES

ACRONYMS AND DEFINITIONS

Table 1: Acronym List

Acronym	Meaning
ACEA	ACEA S.p.A.
ALBLF	Alcatel-Lucent Bell Labs France
CIS-UROME	Università Degli Studi Di Roma La Sapienza
DoW	Description of Work
EPIST	Epistematica SRL
ICT	Information and Communication Technology
IMT	Institut Mines-Telecom
RHEA	RHEA System S.A.
SUPELEC	Ecole Supérieure D'Électricité
UCD	User-centered design
UoL	Universität zu Lübeck
D&E	Dissemination and Exploitation
ESA	European Space Agency
EO	Earth Observation
HPC	High Performance Computing
SCADA	Supervisory Control And Data Acquisition
IRT	Institut de Recherche Technologique
EGS-CC	European Ground Systems - Common Core
CDSA	Cyber Defence Situational Awareness
RFI	Request for Information
NATO	North Atlantic Treaty Organization
SSE	Secure Software Engineering
IPR	Intellectual Property Rights

1 INTRODUCTION

1.1 Purpose

The purpose of this document is to provide information concerning the dissemination methods and exploitation of its results for the needs and goals of the FP7 funded PANOPTESEC Project delivery of prototype technologies supporting Dynamic Risk Approaches for Automated Cyber Defence (PANOPTESEC). It also provides details about the dissemination and exploitation activities to be undertaken during the project as well as an outlook on possible activities after its completion. At this stage, it is not intended that this document provide extensive details of dissemination and exploitation activities or results since these results are otherwise presented in the D8.1.3 Dissemination and D8.1.4 Exploitation Reports.

1.2 Scope of the PANOPTESEC Dissemination and Exploitation Plan

The main purpose of the PANOPTESEC Dissemination and Exploitation (D&E) plan is to provide an overview of the D&E activities throughout the project and support of measuring the D&E results. It also serves as a guideline for actions to be taken by each partner and the consortium as a whole, identifying possible opportunities for D&E activities that will be further build-up during the project development.

The PANOPTESEC D&E activities are coordinated by RHEA, the consortium partner that is responsible for the Task 8.1 Information Dissemination. All participating members of the consortium provide support and participate at the D&E activities as required by the DoW. As leaders of Work Package 8, ACEA has overall responsibility for the Dissemination and Exploitation activities, though development of the Dissemination and Exloitation Plan has been delegated to the Task 8.1 Leaders at RHEA. RHEA is therefore responsible for supporting the PANOPTESEC Steering Committee in decision making regarding the dissemination and exploitation of each outcome of the project and works closely with the project partners ensuring timely and effective communication and interaction with targeted audiences, so that the project results can be optimally exploited.

The D&E's overall mission includes the following activities:

- To support high level dissemination of project results and achieved milestones;
- To keep the public updated via the project website, social media, events and publications; and
- To support the intellectual property rights applications of the partners and to ensure each partners' claim is properly dealt with.

1.3 Document Structure

Following this introductory section, this document is divided into five sections covering aspects of the dissemination and exploitation activities and related schedule. The first section covers the dissemination plans including the main tools and channels that will be used to communicate the major project results. This section is followed by the methodology

that was followed to develop the D&E plan. The following sections provide incremental detail related to actual dissemination details and exploitation plans. The document concludes with a summary of the results and recommendations.

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

Section 2 Methodology: describes the approach for the development of the D&E plan.

Section 3 Dissemination Plans: describes the methodology followed in the development of the Dissemination Plans and how these are being implemented.

Section 4 Dissemination Roadmap: describes the activities in a timeline grid.

Section 5 Exploitation Plans: describes the methodology followed in the development of the Exploitation Plans and how each partner plans to exploit the results of this project.

Section 6 Conclusion: summarises the findings, results and recommendations.

2 METHODOLOGY

2.1 Stakeholder identification

The PANOPTESEC project has identified different types of stakeholders, that is persons or entities that may be affected by or may affect the scope and intended use of the system developed in the PANOPTESEC project.

A detailed description of the stakeholders has been included in the document D2.2.1: Operational Requirements (section 2.1 Stakeholder identification). In brief, the following categories have been identified: 1) client stakeholders; 2) market stakeholders; 3) partner stakeholders; and 4) user stakeholders.

The dissemination and exploitation strategy and plan has been based on the analysis of the stakeholders identified above and assessment of the needs of the cyber security community.

The PANOPTESEC D&E strategy and plan is positioned to achieve the following general dissemination objectives:

1. PANOPTESEC public website: The website will provide all necessary and relevant information about the project and the consortium. As progress is made on each of the component modules, significant findings can be announced via the website for broad distribution;
2. EU project clustering activities: Coordinated by the SECCORD (SECurity and trust COoRDination and enhanced collaboration) project, PANOPTESEC will conduct coordination activities with SECCORD and participate in SECCORD clustering events;
3. Scientific publications and conferences: Scientific publications and conferences provide a recognized means to disseminate results. Each PANOPTESEC partner planned to contribute papers and participate in one industry-relevant conference per year;
4. Project workshops: The project set out to organise two workshops. The first workshop being near or at the end of the component experiments and refinement phase when individual component modules will be in a position to highlight the results of their project contributions in specific areas. The second workshop being at the conclusion of the project when the results of the integrated system could be demonstrated at ACEA.

2.2 Quality assurance

The Quality Assurance (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 Quality Assurance Manager (QAM), validated at a Consortium level and centralised in the Project Handbook.

For the purpose of the QA of the D8.1.2, the deliverable has been assessed according the following checklists:

- PEER REVIEW (PR) QA CHECKLIST: the D8.1.2 deliverable is a report, it then requires a proper peer review according to the checks defined in this checklist.

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

3 DISSEMINATION PLANS

3.1 Dissemination Goals

This plan comprises the necessary and potential key means in the dissemination and exploitation of the project in order to ensure the following:

- The science and technical community as well as other potentially interested audiences will become aware of the PANOPTESEC project, its content, goal and results
- PANOPTESEC will establish a leading role within the Information Security fora, workshops etc. and will build relationships with other FP7 related projects
- Promotion of PANOPTESEC concepts and approaches to target markets relevant to future exploitation activities.
- The PANOPTESEC state-of-the-art technologies will be exploited after the completion of the project.

3.2 Target Groups

The target groups of PANOPTESEC dissemination activities, include the following categories:

- Science and technical community
- EU stakeholders
- Target market stakeholders
- Inter-project representatives
- General audience

3.3 PANOPTESEC Identity

The PANOPTESEC project identity has been established through the use of a distinct logo and document templates.

3.3.1 PANOPTESEC logo

'Panoptes' is an ancient Greek term meaning "all eyes" or "all seeing", and has been incorporated into the project name, PANOPTESEC, to reflect the overall goals of the project.

In Greek mythology, Argos Panoptes was a hundred-eyed giant, who was requested by Hera, the wife of Zeus, to watch over the consort of her husband. After he was slain while performing his duty, Hera posthumously rewarded Panoptes by placing his hundred eyes on the tail of her sacred peacock.

The eyes on the peacock feather have been used in the PANOPTESEC logo, linking Greek mythology with the project concept through both the project name and logo image.

The last three letters at the project name, SEC, link the name of the mythological figure Panoptes with the security domain of the project.

Figure 1: PANOPTESEC Logo

3.3.2 Templates for documentation and presentation

Templates for documentation and presentation have been designed and are available since Month 3 of the project. They have been revised, incorporated in the project handbook and verified through quality assurance after the 1st review.

3.4 Communication Tool and Channels

3.4.1 Project Website

The PANOPTESEC project website (http://panoptesec.eu/) was launched during the first 3 months of the project following the best practice guidelines made available by the EU funding agency for FP7 projects. The project website complements the activities of the PANOPTESEC project through promotion and dissemination of the results and achievements to interested user communities as well as the general public.

There is also a special mobile-friendly version of the website to provide access to its contents using mobile devices (http://panoptesec.eu/mobile).

For details about the project website, please refer to document D8.1.1 Operational Project Website.

3.4.1.1 Website Images

The website has adopted a neutral background of a partly clouded blue sky. All website images (company and academia logos, EU and FP7 logos, technical diagrams, tables, etc.) are in standard image formats (jpg, gif, png), with transparent backgrounds where appropriate.

3.4.1.2 Web Domain

The web domain selected for the project website is www.panoptesec.eu, following best practice guidelines defined for EU project websites. The domain name has been registered for five years, covering the full three years of the project duration, plus an extra two years.

3.4.1.3 Technical Principles

The PANOPTESEC website adopts standard web technologies for the construction of the website. These include HTML, SHTML, Cascading Style Sheets (CSS) and JavaScript applets.

3.4.1.4 Design Principles

The project website is designed for easy maintenance, separating different content sections into different directories, and employing Server Side Include (SSI) files for repeatedly used

content areas, such as headers and footers. A horizontal pull down menu is employed to facilitate navigation.

3.4.2 Social Media

3.4.2.1 LinkedIn Group

The PANOPTESEC LinkedIn Group (https://www.linkedin.com/groups/PANOPTESEC-Cyber-Security-Project-7461693/about) was created during the first months of the project. This group has been used to promote the PANOPTESEC news and also create an area for open discussion about related cyber security topics, further establishing the project's presence in this domain.

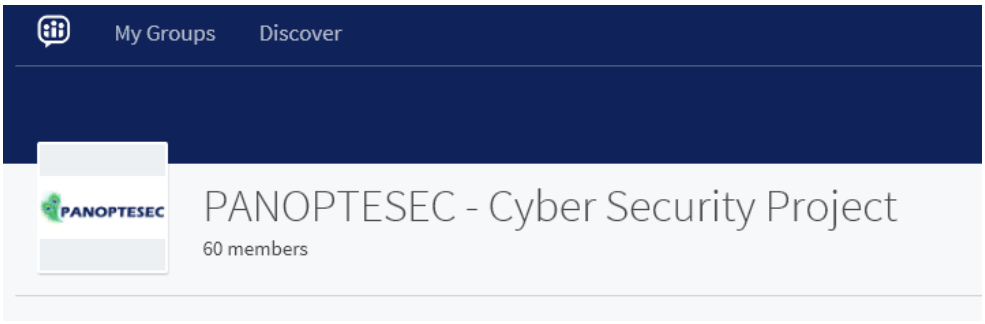

Figure 2: PANOPTESEC LinkedIn Group Banner

The PANOPTESEC LinkedIn Group The group is open to visitors who wish to read its content but it requires moderator acceptance for membership. Publication of posts and, in general any information, is supervised by the group moderators to ensure that there is no spam or stale information. Currently, there are 138 members in the group. This number has increased incrementally after various project events. These events have also resulted in traffic coming back to the website.

The LinkedIn Group has been an effective tool to promote project dissemination activities.

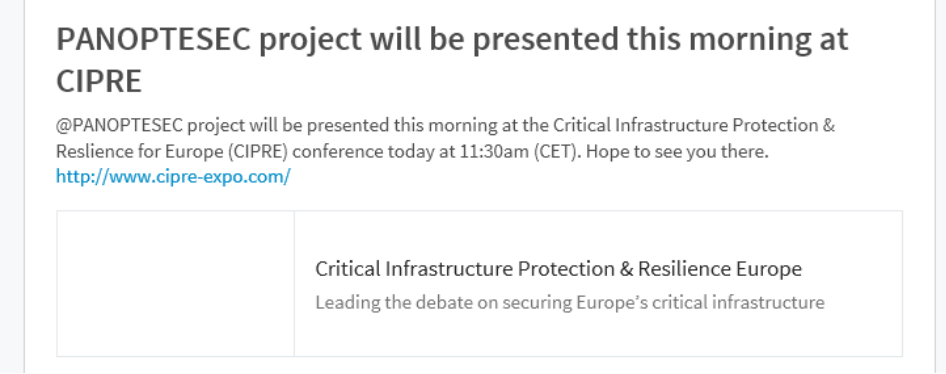

Figure 3: PANOPTESEC LinkedIn account use to promote project activities

Statistics of the LinkedIn Group activity for the duration of the project are provided in Figure 4 (updated at 26/10/2016):

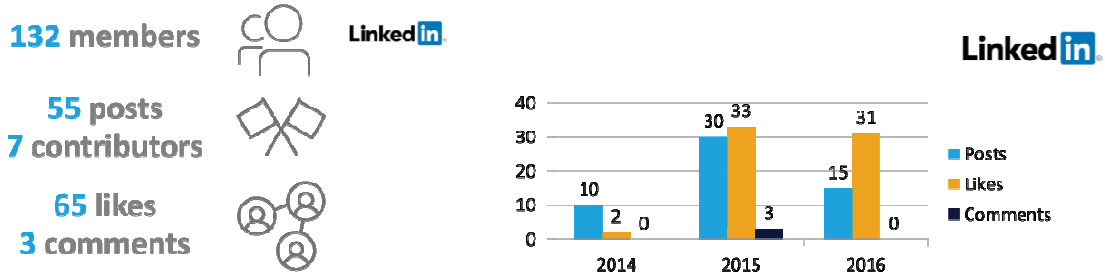

Figure 4: PANOPTESEC LinkedIn Group statistics

3.4.2.2 Twitter Account

In addition to the PANOPTESEC LinkedIn group, PANOPTESEC has established a dedicated Twitter account. This account is used to promote ongoing activities of the project and comment on news and events related to cyber security.

Figure 5: PANOPTESEC Twitter account

The Twitter account is intended as effective tool to further promote dissemination activities. For example participation in the Critical Infrastructure Protection for Europe (CIPRE) conference was promoted through the twitter account. In particular the Twitter account was effectively used during the Operational Workshops to promote and advertise the event.

Figure 6: Twitter account used to promote project operational workshops

Use of the Twitter account takes further advantage of extended social media links as followers of the group can 're-tweet' the PANOPTESEC announcements. This is supported by project partners who publish news in their social media accounts. As can be seen in the example below, the PANOPTESEC presentations dissemination events are re-tweeted by various partners and third-parties as illustrated in Figure 7.

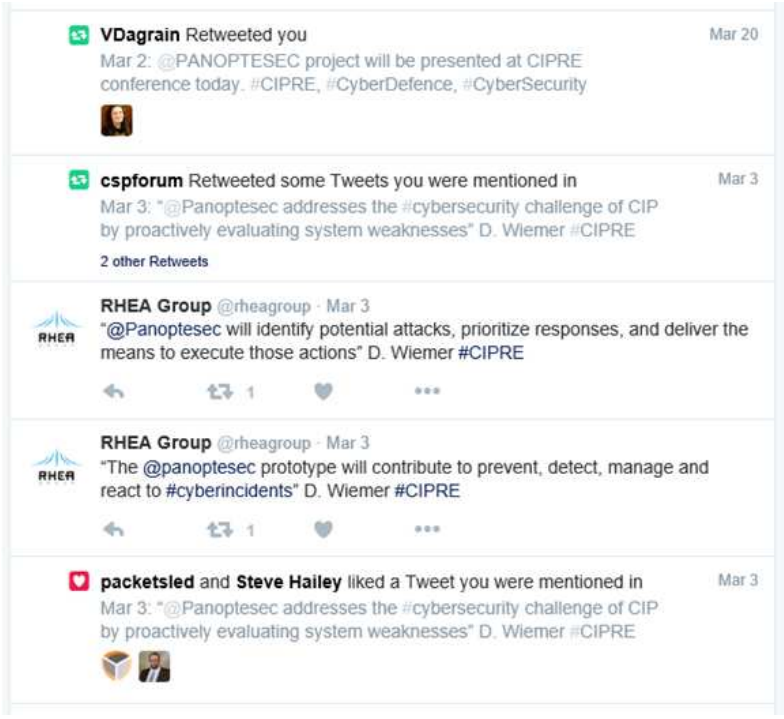

Figure 7: Twitter account activity is promoted by partners and other parties

Statistics of the Twitter Account activity and related re-Tweets on other accounts for the duration of the project are provided in Figure 8.

Figure 8: PANOPTESEC Twitter statistics

3.4.3 Publications and Conferences

Each PANOPTESEC partner plans to contribute papers and participate in at least one relevant conference per year. These contributions are coordinated between partners such that the collaborative nature of the PANOPTESEC consortium will be promoted to the industry and the cyber defence research community. In addition, the PANOPTESEC project will benefit from the visibility that publications focusing on cyber security and related technical developments can offer. Project partners place intentional focus on peer reviewed scientific publications, in addition to more general publications and conference events.

Recognizing the importance of raising industry awareness, the dissemination strategy also involves participation in high profile industry conferences targeting the cyber security community. Some example conferences include:

- Critical Infrastructure Protection and Resilience for Europe (CIPRE 2016); and
- Information Security Europe (InfoSecurity Europe 2016.

In addition to the press releases published in the project's channels (website and LinkedIn group), the dissemination of the project's results are realised via technical and general publications, newsletters, conference proceedings and associated websites.

A comprehensive list of resulting publications and conferences is provided in the D8.1.3 Dissemination Report.

3.4.4 Press reviews

In addition to publications and conferences, the dissemination strategy involves leveraging a variety of news channels and press reviews to give the project good external visibility. The project targets is at least 5 such press reviews, with focus towards the end of the project when project results can be actively promoted, creating interest as part of the transition from dissemination to exploitation.

3.4.5 Project workshops

According to the PANOPTESEC Description of Work (DoW) it was intended that two workshops be organised by the Consortium. The first workshop was intended to be near or at the end of the component experiments and refinement phase when individual component modules would be in a position to highlight the results of their project contributions in specific areas. The second workshop would be at the conclusion of the project when the results of the integrated system will be demonstrated on an operational segment of a critical infrastructure provider (ACEA).

The project has expanded on this initial goal by including the following workshops as part of the dissemination and exploitation strategy and plan. Details of these workshops are reported in the D8.1.3 Dissemination Report:

1. Mid-project workshop #1: A 2-day project workshop on 8-9 September, 2015 conducted in Brussels and hosted at the Diamant Business and Conference Centre. The workshop was conducted in collaboration with the H2020 PaaSWord project. The focus of the workshop was split each day, with Day 1 having focus on Cloud service providers and SMEs, while Day 2 was focused on agency level and large enterprise organizations. Each project had the opportunity to present their overall project concepts and approach. The PANOPTESEC project then provided detailed demonstrations of project status.
2. Mid-project workshop #2: The project conducted a half-day security workshop as part of the InfoSecurity Europe Conference held in London, 7-9 June, 2016. This workshop also provided the opportunity for the project to host a project booth over the three days in the Innovation Zone, allowing increased opportunity for project members to interact with conference participants.
3. Final operational workshop: The operational workshop was held in ACEA premises from 17th to 28th October, 2016. The operational workshop was hosted on the disaster recovery segment of the ACEA operational network. The workshop itself was organized in 16 sessions in order to facilitate interaction with a range of external stakeholders. The operational workshop was promoted through an extensive campaign of invitations and organized using an EventBrite registration mechanism. The invitations were extended to a range of industries including Public Utilities; Information Technology; Banking and Finance; Defence; Telecommunications, Television and Transportation and involving both from small to medium enterprise (SME) and large enterprise. The presentations were first prepared as part of the Milestone 7 Qualification Review activities, including demonstrations of the

operational software to both internal stakeholders from ACEA and also to the External Advisory Board. A full description and the results of feedback of the operational workshop are described in Deliverable D8.2.3.

3.4.6 Collaboration with Organisations and Synergies with other Projects

Opportunities to network with other projects and partners are considered, to ensure wherever possible that there is knowledge interchange between projects. To this end, the PANOPTESEC seeks to exchange and leverage with relevant European or national funded research programmes where possible.

In this area, the project has maintained interactions with the following organizations and projects:

- EU FP7 project SecCord (http://www.seccord.eu) prepares for the EC an annual yearbook providing an overview of the major research and innovation achievements of the FP7 Trust and Security Programme. PANOPTESEC has been included in the EU Yearbook 2014 - FP7 project SecCord. PANOTPESEC has also been included in the SecCord publication highlighting "Contributions of the FP7 Trust & Security projects towards the EU Cybersecurity Strategy" in 2015.

  http://www.cspforum.eu/Annex_4_Contributions_to_EU_Cyberstrategy_copy.pdf

- The PaaSword project participated in the first mid-project operational workshop organized by PANOPTESEC in Brussels in September 2015.

- Following participation in the Critical Infrastructure Protection & Resilience for Europe (CIPRE) conference, June 2016, the project took steps to establish collaboration with the PRE-EMPTIVE project. The PRE-EMPTIVE Project places emphasis on sensor data collection in critical infrastructure environments. Due to the early stage status of the PRE-EMPTIVE project, collaborative opportunities have been limited, but will be pursued as part of project follow-up activities;

- ACEA promoted the PANOPTESEC project within the FP7 Security Project ECOSSIAN "European COntrol System Security Incident Analysis Network" (www.ecossian.eu) through the Consortium partner Poste Italiane SpA;

- ACEA promoted the PANOPTESEC project within the H2020 Project SUCCESS "securing critical energy infrastructures (www.success-energy.eu/) through the Consortium partner ASM Terni SpA;

- ACEA promoted the PANOPTESEC project within the FP7 C2-SENSE "Interoperability Profiles for Command/Control System and Sensor Systems in Emergency Management" (www.c2-sense.eu) through the Consortium partner Lutech SpA.

3.4.7 Official EU Dissemination Channels

The project PANOPTESEC is participating to clustering and community building activities supported by the European Union in the area of cybersecurity and/or trustworthy ICT. It will actively engage in dialogues with relevant stakeholders including policy makers, industry

and academia, and thereby contribute to the shaping of the Union's cybersecurity policies, industrial strategy and research area. Public deliverables will be made available to the Commission for publication on the Commission web site and other communication channels.

The following dissemination activities are particularly noteworthy:

- May 20, 2014: Participation by D. Wiemer (RHEA) at CSP forum - Athens, Greece
- June 18-19, 2014: Participation by A. Guarino (ACEA) in “Security Summit 2014”, organised by AIIC-Clusit
- July 3, 2014: Participation by A. Guarino (ACEA) in “First National Conference on Cyber Security for the Energy Sector-2014”, organised by EnergyMedia – World Energy Council (WEC)
- October 15, 2014: Participation by A. Guarino (ACEA) in “CyberSec 2014 event”, organized by Intel Security
- November 5, 2014: Conference participation by M. Merialdo, G. Mihalachi and K. Zidoune (RHEA) at the SECONOMICS Summit (Security Economics for Critical Infrastructure) – Brussels, Belgium
- March 2-3, 2016: The PANOPTESEC project was presented at the Critical Infrastructure Protection & Resilience for Europe (CIPRE) conference – The Hague, The Netherlands.

4 DISSEMINATION ROADMAP

4.1 First Year Dissemination Activities

Dissemination activities carried out in the first year of the project included:

- designing the project logo
- setting up the project website
- setting up the project website mobile-friendly version
- setting up the social media presence
- sending out first press releases
- participating in relevant conferences, information day events, workshops and present PANOPTESEC objectives and first milestones
- spreading the word of PANOPTESEC activities in every suitable context (by all partners)
- evaluating further dissemination activities

4.2 Second Year Dissemination Activities

Dissemination activities carried out in the second year of the project include:

- extending the project website
- maintaining and posting news on the LinkedIn group
- promoting the project on conferences and events
- promoting the project to relevant organisations, companies and other stakeholders representing target markets relevant to future exploitation activities
- submitting papers to academic journals
- workshops to support market validation and overall dissemination

4.3 Third Year Dissemination Activities

Dissemination activities carried out in the third and final year of the project will include:

- Promoting the project on conferences and events focusing on exploitable results
- Submitting papers to academic journals and engaging with the extended target audience, creating a detailed exploitation plan for the final project results
- Coordinate two workshops; one workshop near or at the end of the component experiments and refinement phase to highlight the results of the project contributions in specific areas (e.g., workshop conducted at InfoSecurity Europe 2016), and another workshop at the conclusion of the project for the demonstration of results in the disaster recovery segment of the ACEA operational network (conducted from 17-28/10/2016). Both workshops are meant for external audiences and key stakeholders.

- Increasing the level of marketing towards relevant organisations, companies and other stakeholders representing target markets relevant to exploitation activities.

4.4 Dissemination Activities after the Project End

The project's work and results will continue to be part of the dissemination activities by all partners whenever the context allows it. It is possible that publications will continue to include results related to the PANOPTESEC project. Also, the project website will remain online for at least two additional years and the project partners can individually update further project results. Last, the project's social media channel will also stay online and open for posting further relevant discussions on Cyber Security and PANOPTESEC.

5 EXPLOITATION PLANS

5.1 Indicative exploitation plans

The PANOPTESEC consortium exploitation plan represents the collective intent of the PANOPTESEC consortium to pursue the results of the project to the maximum extent possible.

To succeed its main goal, the PANOPTESEC project will provide a prototype, which implies that the exploitation possibilities are significant. This system will be first used by ACEA, one of the largest Italian public utility companies for power and water supply.

The consortium as a whole and each partner separately has already identified and foresee various ways that the results can be further exploited by the project completion and beyond (please see section 5.3 below). Depending on each partner's profile and business objectives, the exploitation of the results may vary from educational transfer and know-how improvement to developing new technologies, products and services. Active research in the areas of visual analytics, cyber defence / cyber security, data analysis will be leveraged for teaching and further research activities as well as real-world applications and commercial service packaging. It is also envisioned that the PANOPTESEC project results will have implications in various security related standards activities as well as security related policy developments.

5.2 Intellectual property rights

PANOPTESEC intends to produce knowledge that can be turned into significant commercial value. The Steering Committee will encourage project partners to protect the knowledge generated and to promote it in standardisation, publications, workshops and conferences. Intellectual Property Rights (IPR) application for new concepts and solutions will be regulated by the concerned participants through the PANOPTESEC consortium agreement, which defines the rules for the ownership and access rights of knowledge.

The PANOPTESEC Project has an established and agreed consortium agreement setting out the rules and requirements for intellectual property ownership, access, confidentiality and responsibilities for protection.

These are the focus areas where involved partners are particularly encouraged and expected to develop and protect intellectual property, including:

- Improved network and security multi-sensor data integration and correlation using a mathematical framework and mixed-initiative problem solving based on Semantic Web technologies;
- Automation of attack awareness and risk assessment via attack modelling taking into account the evolution of systems and services, the emergence of new threat sources and newly discovered system vulnerabilities, and the operational mission priorities;
- Automation of attack awareness and risk assessment via risk quantification through data collection, threat assessment and risk modelling;

- Automation of attack awareness and risk assessment via decomposition of risk quantification into separate proactive and reactive assessment chains;
- Automation of response assistance to provide cyber defence operators with prioritized courses of action recommendations for review and activation;
- Advanced mechanisms to capture and model mission/business process relationships to services and systems based on Semantic Web technologies; and
- Advanced visualization techniques for mission/business process risk display including representation

Within the D&E activities, eventual intellectual property rights applications will be supported, ensuring each partner's claims.

A complete list of resulting project outputs is provided in the D8.1.4 Exploitation Report.

5.3 Commercial partner-specific exploitation plans

This chapter describes the PANOPTESEC exploitation plan identified by each commercial partner of the Consortium.

5.3.1 PANOPTESEC Exploitation by RHEA

5.3.1.1 Partner profile and background

Since 1992, RHEA has been providing space engineering services and products to the international space community including the European Space Agency (ESA) and EUMETSAT. RHEA is the proud supplier of the Mission Operations Information System (MOIS) technology, used in support of over 100 space missions and also a leading provider of concurrent design and engineering systems and services with its flagship product, Concurrent Design Platform™. With headquarters in the Brussels area of Belgium, RHEA is an international organisation with an established presence in Belgium, the Netherlands, Italy, Germany, Spain, Switzerland, the UK, the Czech Republic and Canada.

Since 2004, RHEA has been broadening its service offerings by taking a strategic approach to the delivery of system and software engineering solutions dedicated to the aerospace, defence and security domains with a particular emphasis on space systems engineering, cyber security, critical infrastructure protection and information technology solutions. Part of this strategy has been the creation of the RHEA Security and Crisis Management (SCM) business unit, providing information security services to agency-level organisations throughout Europe. It is the mission of the RHEA security practice to deliver innovative solutions to meet security applications, systems and operations requirements. Most recently, in December 2014, RHEA acquired majority shareholding interest in SixSq, a European leader in Cloud Computing technologies and services.

5.3.1.2 Exploitation strategy and early results

As a SME industrial partner within the PANOPTESEC consortium, RHEA will pursue commercial opportunities for delivery of PANOPTESEC as a productised solution for cyber defence in the following markets:

1. Space Systems Security: Space systems are more and more recognised as critical infrastructures. These environments have similar requirements for security monitoring other critical infrastructure and national defence environments. RHEA has several initiatives already underway that leverage PANOPTESEC results in the domain of Space Systems Security.
    a. European Security Certification Standards for space assets: In response to the ESA GOVSATCOM Precursor Activities, RHEA has submitted a Notice of Intent to submit an Outline Proposal. This proposal presents a recommendation to establish a European Space Security Certification Scheme (ESSCS) and independent security evaluation facility. Additional details are provided in D8.1.4 Exploitation Report;
    b. Space Systems and Solutions: ESA are developing a common approach to ground system solution and delivery called the European Ground Station Common Core (EGS-CC). RHEA has been actively involved in the EGS-CC prototyping efforts and is the Belgium Prime for involvement in EGS-CC testing framework. Although operating in different industrial domains, the EGS-CC and the PANOPTESEC Integration Framework share common technologies and approach. This is an intentional step by RHEA to leverage common results between the two projects.
2. Critical Infrastructure Protection: A primary customer opportunity for PANOPTESEC, RHEA is promoting the concepts to potential public and private utilities companies (energy, water, oil & gas, etc.). Recent media coverage demonstrates growing concern over the issues of cyber-attacks to critical infrastructure[1]. RHEA has intentionally established a Critical Infrastructure Protection Business Strategy targeting this market on a regional basis where infrastructure providers are being approached and presented with PANOPTESEC as packaged solutions. Specific opportunities within this market include participation in the proposed Multi-sector National Testbed for Critical Infrastructures[2] as part of The Hague Security Delta in The Netherlands. It is intended that RHEA capabilities for delivering a critical infrastructure emulation environment similar to PANOPTESEC emulation environment will be leveraged into the National Testbed. RHEA is also participating in a proposal to the European Space Agency as part of the Integrated Applications Programme (IAP) in which the PANOPTESEC system will be used to secure a crisis management and response infrastructure for industrial accidents according to SEVESO[3] regulations;

[1] Matgen, Le Bussy, Braun, Lambrecht, and Lovens, http://www.lalibre.be/actu/belgique/attentats-d-ici-5-ans-ils-pourraient-prendre-le-controle-d-une-centrale-nucleaire-56f58f4d35708ea2d3e8e878, La Libre.BE, 26/03/2016, last accessed 04/04/2016.
[2] The Hague Security Delta, "Securing Critical Infrastructures in the Netherlands: Towards a National Testbed," https://www.thehaguesecuritydelta.com/images/HSD_rapport_Testbed_EN.pdf, 2015, last accessed 04/04/2016.
[3] http://ec.europa.eu/environment/seveso/

3. Cloud Provider Security: RHEA has majority interest in SixSq, an innovative provider of technology and solutions for automated provisioning of cloud services. PANOPTESEC is considered a valued added solution for cloud provider environments, offering a large scale capability for continuous security monitoring. Increased capabilities for continuous security monitoring in cloud environments may improve market opportunities for Small-Medium Enterprise (SME) that may otherwise be reluctant to take advantage of cloud provider services. SixSq are actively involved in projects related to security of industrial control systems, critical infrastructure, and secure cloud delivery (H2020 projects: SCISSOR, CYCLONE and PaaSword). The combined technology opportunities of these projects towards increasing cloud provider security and supporting their SME clients is a significant market for RHEA;
4. National Defence Organisations: Due to the evolution of the cyber threat, national defence organisations must pursue advanced solutions to counter the threat. Some already identified business opportunities include the Cyber Situation Awareness Package (CySAP) within the European Defence Agency (EDA) and the Cyber Defence Situational Awareness (CDSA) work package within the NATO Multi-national Cyber Defence Capability Development (MNCD2) project. Leveraging the PANOPTESEC experience, RHEA submitted a proposal on 4 November 2016, to the EDA CySAP project, in collaboration with partner UROME. If successful, the project will involve definition of the System Requirements and Target Architecture of the future CySAP project.

As a SME industrial partner within the PANOPTESEC consortium, RHEA has already achieved some successful exploitation of PANOPTESEC results and will continue to pursue commercial opportunities for delivery of PANOPTESEC as a productised solution for cyber defence.

Leveraging corporate capabilities and experience developed within the PANOPTESEC project, RHEA has successfully proposed and been awarded a contract with the European Space Agency (ESA) to deliver a “Cyber Security Training Range” at ESA Station in Redu Belgium. The value of the contract is € 480 K and has a mandate to deliver a virtualized technical environment supporting a variety of cyber security related training, research, development and test activities in a relevant space assets simulation context. The project will also deliver a Long Term Perspective, with recommendations for ongoing use of the facility beyond the current project. This provides additional potential for expanding business at RHEA. RHEA experience in delivering the PANOPTESEC emulation environment not only improved corporate capabilities in this area but was also a substantial factor in the successful evaluation of the RHEA proposal as a reference project.

Following the success of the Operational Demonstration Workshops at ACEA in October 2016, RHEA has been approached by several companies interested to have deeper understanding of PANOPTESEC technologies for future exploitation. At this stage it is too early to determine the full scope of the opportunities, however each represents potential for product related sales, embedded product licensing, or technology support services. Additional detail of these opportunities is provided in the D8.1.4 Exploitation Report.

5.3.1.3 Product Packaging and Branding

Following the success of the ESA Cyber Range, RHEA will continue to pursue opportunities in the various core markets, incrementally developing productized versions of the PANOPTESEC solution according to the modular and packaged outputs described in Section 3.2 of the D8.1.4 Exploitation Report.

As part of project closure activities, RHEA is further refining the packaging approach and developing a branding strategy. Additional market assessments specific to key regional priorities of RHEA are underway with particular focus in Belgium and Italy. In support of this, RHEA has recently hired a new General Manager for RHEA in Italy and augmented the business development team with additional resources in Belgium. In both cases, these additional business development resources have a particular focus towards development of exploitation opportunities for PANOPTESEC outcomes.

The RHEA Group security product branding strategy is intended to capture several core concepts of the PANOPTESEC, while providing a unique brand characteristic of the RHEA Group.

5.3.1.4 Risks and mitigation strategy

The main risk envisioned for RHEA exploitation of PANOPTESEC is that the technical achievements of the project are too complex or comprehensive for market acceptance of the complete solution. This risk is mitigated by the packaging options identified in the D8.1.4 Exploitation Report. These packaged outputs provide the opportunity to deliver specific components in an incremental way, supporting a staged roadmap of delivery.

Also, as a systems integrator, RHEA is focused on delivery of a robust integration framework as part of the PANOPTESEC solution. This framework is built on a strong system engineering approach supporting commercial release. The modular nature of the framework supports further component refinement or integration of alternate commercial modules according to market demand. This approach provides a solid basis for successful commercial release.

5.3.1.5 Implementation strategy

The implementation of our exploitation strategy includes the following:

1. Market driven materials: In support of business development activities, RHEA will prepare PANOPTESEC based marketing materials including white papers and case studies under a new product brand. This will prepare customers for interest in the resulting packaged solution and component parts. A combined RHEA-SixSq eGuide “Smart City Cyber Protection for Critical Infrastructures” has already been produced to highlight the use of the SixSq Nuvlabox in the PANOPTESEC project as a cyber security sensor host platform in remote critical infrastructure facilities (e.g. electricity distribution substations);
2. Technology demonstration events: RHEA actively participates in industry conferences and demonstrations in relevant market segments. Trade exhibits within the industry conferences will provide significant opportunity to showcase PANOPTESEC results;

3. Expansion of existing client contracts: As noted above, existing clients (e.g., ESA, EDA and NATO) have significant requirements for cyber defence continuous monitoring solutions. RHEA has already begun promoting PANOPTESEC concepts to existing clients in order to generate interest and new business opportunities and has seen early successes. Although not specifically a cyber security related project, RHEA is leveraging common aspects of the integration framework between the PANOPTESEC and EGS-CC projects; and
4. Active bidding on upcoming opportunities: The ESA Cyber Range project demonstrates early success for RHEA in this area. As noted above, upcoming opportunities fit the PANOPTESEC scope and concepts (e.g., ESA GOVSATCOM and EDA CySAP). RHEA is well positioned to propose a PANOPTESEC-based solution as the winning approach to meet these and similar requirements. RHEA has submitted an Outline Proposal to the ESA GOVSATCOM Precursor Activities on 06/05/2016. RHEA has also submitted a proposal for improving cyber security of space assets as part of the ESA ARTES 5.2 programme and is currently preparing a proposal as part of a consortium towards the ESA IAP for security of infrastructures supporting crisis management.

5.3.2 PANOPTESEC Exploitation by Alcatel-Lucent (ALBFL)

5.3.2.1 Partner profile and background

Alcatel-Lucent is at the forefront of global communications, providing products and innovations in IP and cloud networking, as well as ultra-broadband fixed and wireless access to service providers and their customers, enterprises and institutions throughout the world. Underpinning Alcatel-Lucent in driving the industrial transformation from voice telephony to high-speed digital delivery of data, video and information is Bell Labs, an integral part of Alcatel-Lucent, responsible for countless breakthroughs that have shaped the networking and communications industry. Alcatel-Lucent Bell Labs France (ALBLF), the French Bell labs centre and the second in size, located in Nozay, close to Paris, is a 100% affiliate of Alcatel-Lucent International and is covering research on optical components, transmission systems and optical networks, ultra-broadband wireless architectures, networking algorithms and protocols, security of communication systems, mathematics of dynamic networks, content oriented networking, Internet of Things, network energy, IP platforms and software for telecoms. Alcatel-Lucent Bell Labs France is active in "pôles de compétitivité" System@TIC Paris-Région and Cap Digital as well as in a number of national and European collaborative projects. Several joint research laboratories were created in France with Alcatel-Lucent Bell Labs France contribution (the III-V lab, a laboratory with INRIA, and the LINCS). Alcatel-Lucent Bell Labs France is also among the leaders of the French node of "EIT ICT Labs" and is also member of the "SystemX" IRT.

5.3.2.2 Exploitation results and strategy

As the research and innovation entity of a huge multinational company, Bell Labs establishes scientific and technological assets in defined strategic research domains with the objectives to uphold, enhance, or incubate markets opportunities for the Alcatel-Lucent Corporation worldwide.

As a long lasting research entity (i.e. more than 120 years of existence) The Bell Labs' mission is to resolve big scientific and technological locks in the Communication and Information Technologies for the profit of Alcatel-Lucent but also for the progress of the knowledge per-se.

Studies in cyber security of current and future networking infrastructure (i.e. cloud networking) performed by Bell Labs, and particularly in the frame of the PANOPTESEC Project are aligned with Bell Labs mission and its exploitation strategy, which is directed toward several axes:

1. Assess the opportunities of established results to be transferred into existing Alcatel-Lucent current and future network solutions and services in order to enhance their cyber security posture. This objective is mainly achieved through the development of prototypes ready for experimentation and industrialization;
2. Establish evaluated and validated prototypes solutions and technologies in the cyber security of current and future network solutions and services that will further be pushed for licensing by Alcatel-Lucent;
3. Develop the Alcatel-Lucent Intellectual Property in the cyber security that could provide a market differentiator to Alcatel-Lucent by providing more secured network solutions and services;
4. Dissemination of discoveries, knowledge, scientific results and technologies through publications in journals (notably, the Bell Labs Technical Journal), conferences, and workshops.

The management of the security of network solutions and services is well established asset in the Cyber Security Research department of Bell Labs for more than 10 years, with several success in the Continuous Security Assurance monitoring and enforcement, and in the Dynamic Risk Management of networking infrastructures. Bell Labs with its Cyber Security Research department holds several tens of scientific papers and patents in the network security monitoring. Several prototypes have been produced during the past 10 years in this field with already successful transfers to CTO and Business Divisions in the domain of Managed Services. We intend to enhance the Bell Labs technology portfolio in the management of network security in the perspective of internal exploitation to enhance Alcatel-Lucent network solutions and service security posture or for licensing.

5.3.2.3 Risks and mitigation strategy

The main risk envisioned for ALBLF exploitation of PANOPTESEC is that the technical achievements of the project do not meet objectives to experiment and validate the resulting solution on a sufficiently significant use case to demonstrate the value of the produced prototypes and intellectual property to go toward a commercial exploitation. Nevertheless, ALBLF still has the conviction that the ACEA use case provides an ideal environment to validate the results of the developed prototype. As a solution provider, ALBLF is focused on delivery of efficient and useful prototypes of functions which enable the dynamic risk management of a monitored system. The concepts, architectures, and algorithms are built on strong scientific and technical basis that need to be experimented and validated on a

sufficiently significant use case to assess their applicability, performance and efficiency in real conditions. The accurate and precise design of ALBLF provided component prototypes and interfaces, agnostic from the underlying use case infrastructure that will be used in PANOPTESEC for experimentation, should enable to adapt them rapidly to another use case infrastructure or test bed. The flexibility of the Data Collection and Correlation Interface, combined with the modularity of the analysis components developed by ALBLF ensure the prototype can operate in this agnostic manner.

5.3.2.4 Implementation strategy

The implementation of our exploitation strategy includes the following:

1. Participate in the publication of papers and articles to scientific venues (journal, conference or workshops) with relevant and convincing experimentations;
2. Demonstrating our prototypes and its usefulness to Alcatel-Lucent customers, internal Business Divisions, French and other countries' governmental entities (i.e. Bell Labs FutureX Days, dedicated demonstration sessions)
3. Assessing the licensing opportunity of our prototypes though Bell Labs technology incubation and licensing entity (i.e. Bell Labs FutureX Labs);
4. Protect Alcatel-Lucent Intellectual Property with patenting of Bell Labs established results.

Further industrial exploitation plan of the project results cannot be provided before the finalization of the merger recently announced by Alcatel-Lucent and Nokia (i.e. 15 April 2015, http://www.alcatel-lucent.com/fr/presse/2015/nokia-et-alcatel-lucent-se-rapprochent-pour-creer-un-leader-des-technologies-innovantes-dans-les) that should be completed during the first half of 2016.

Once the merger between Alcatel-Lucent and Nokia completed, any further elaboration of the exploitation plan will be included in D8.1.4 "Exploitation Report" or is otherwise considered Alcatel-Lucent Bell Labs France proprietary and is not intended to be provided.

5.3.3 PANOPTESEC Exploitation by Epistematica Srl

5.3.3.1 Partner profile and background

Epistematica Srl operates in the design of knowledge-driven systems for industrial applications. Epistematica has specific expertise in the use of Semantic Technologies for Knowledge Representation and Automated Reasoning. In this area, Epistematica has competencies in Description Logics and all the Semantic Web technologies. Epistematica offers innovative services and products to design and implement original solutions that provide value and several advantages compared with traditional applications based on syntactic technologies and single-node computing.

In recent years, Epistematica has focused on providing knowledge-based systems for the space industry, with the aim of providing easier data integration, correlation and access to EO data by non-expert users. Epistematica has been so far involved in five ESA projects:

each project has been a step forward in the direction of adopting ontology-based application and reasoners to make the discovery and retrieval of EO resources easier for end-users.

Epistematica also performs research in Robotics, Cyber Security, Cultural Heritage, Digital Libraries, Earth Observation, and Financial Reporting.

Epistematica develops Knowledge-driven Systems using its own products, open-source products and several frameworks to manage and visualize data; uses automated reasoners to retrieve knowledge; uses NoSQL Databases management systems for its systems; develops in Concurrent Programming for multi-node environment (HPC); uses Hadoop Distributed File System for running its Big Data applications.

Epistematica provides courses on Knowledge Engineering at the University of Rome.

5.3.3.2 Exploitation results and strategy

In the academic side, Epistematica will perform dissemination of scientific knowledge through short courses and conferences, in the applied semantic technologies to information security domain.

Within Work Package 4, Epistematica is performing a research activity in the field of ontology-enabled reachability matrix correlation. Epistematica aims at performing a commercial exploitation of this component in two ways: by selling the components developed by Epistematica within the PANOPTESEC system together, and by selling sub-components of general purpose use in other fields of application.

5.3.3.3 Risks and mitigation strategy

An identified risk is the rapid evolution of technology and the uncertain future data formats to deal with. A mitigation of this risk is to design the component in an abstract way so as to be able to process any future kind of input data.

5.3.3.4 Implementation strategy

A first step is to perform dissemination, presenting the results in conferences like:

a) related to topics where Semantic Technologies and Cyber Security converge, for example: SEMANTIC TECHNOLOGY FOR INTELLIGENCE, DEFENSE, AND SECURITY (STIDS), http://stids.c4i.gmu.edu/
b) Application of ICT to Privacy and Data Protection Management:
   - IAPP Europe Data Protection Congress 2015 - https://privacyassociation.org/conference/iapp-europe-data-protection-congress-2015/
   - International conference Computers, Privacy and Data Protection 2016 - http://www.cpdpconferences.org/index.html

The implementation of Epistematica's exploitation strategy will be performed through establishing a "Spin-off" company. In accordance with the Panoptesec project Consortium Agreement - PPCA, IPR and access rights chapter, Epistematica decided to create a new company to exploit its own results of the publicly-funded research.

It will be an European simplified company based on the Italian regulatory. The share of the company will be open to the authors, contributors (e.g., Tech evangelists) and stakeholders, as well as to the partners of the PANOPTESEC consortium.

The rationale for Epistematica to establish a spin-off company are based on the current company focus, compared to the needs of PANOPTESEC exploitation. Epistematica is specialized in research, design and development of solutions based on semantic technologies. It is not a cyber-security or software firm. To take advantage from the research it was decided to create a new company together with domain experts. Further, software solutions like the Reachability Matrix Correlator, designed and developed by Epistematica to compute reachability matrix with a semantic approach, are not yet in the market.

The business model of the new company will be digital, fully inside the digital economy paradigm. Additional details of the Epistematica approach towards the spin-off company are provided in the D8.1.4 Exploitation Report.

5.4 PANOPTESEC exploitation for end-user partners

The PANOPTESEC consortium includes one partner which represents the end-users of PANOPTESEC-like solutions.

5.4.1 PANOPTESEC Exploitation by Acea

5.4.1.1 Partner profile and background

Among the most important Italian public utilities, Acea is an industrial Group which focuses on the consolidation and creation of value from its two main activities, energy and water. Stock market listed since 1999, it deals with the management of energy, environmental and water services: the production, sale and distribution of energy, the development of renewable sources, the disposal and creation of energy from waste, the public and artistic lighting, and an integrated water service (aqueducts, sewerage and purification). Acea has always taken seriously its corporate social responsibility, and pays particular attention to all stakeholders, profitability, service quality and sustainable development. Being a prominent Critical Infrastructure utility, both for water and electricity, the Acea Group has a strong focus on Cyber Security and actively participates in working groups, projects and public events.

5.4.1.2 Exploitation results and strategy

Acea Group intends to use the PANOPTESEC system to actively monitor and protect its SCADA Command & Control centres and ICT environments to defend them from Advanced Cyber Threats: being the only User Agency of the PANOPTESEC project, Acea Group will use its test bed to validate the results of the system and then move it to the production environment.

Moreover areti (former Acea Distribuzione) confirmed in the budget resource allocation for the year 2017 the extension of the IT and SCADA protection systems to the main electricity distribution sites, closely followed by the integration with the PANOPTESEC system (value: 60K euro investment for 2017, plus ordinary maintenance/licence renewal costs).

5.4.1.3 Risks and mitigation strategy

The main risks envisioned for Acea exploitation of the PANOPTESEC are related to the interactions with the existing systems and operators, the responsiveness of the system and the quality of the results obtained from it: as an example, if the rate of false positives will be too high (i.e. over the expected results), the cost in terms of time and resources needed to properly analyze, categorize and solve them could not be tolerable and we could be forced to revert to other solutions. To mitigate these risks, Acea team closely monitored the results and performances regularly during the development, avoiding or solving conflicting situations in advance. To avoid any unwanted interaction, a dedicated room is available in ACEA Headquarters to showcase the system functions in a simulated but real protected environment, without introducing any risk in the functional operational context.

5.4.1.4 Implementation strategy

The implementation strategy includes:

1. After internal validation, testing the PANOPTESEC system in our real-world contexts (i.e. Acea Distribuzione);
2. Giving access to our partners and other selected parties to our premises for the demonstration of the PANOPTESEC system;
3. Organisation and/or participation to national/international events related to Critical Infrastructure Cyber Protection;
4. Participate and present PANOPTESEC outcomes to additional seminars and workshops for further dissemination and networking;
5. Actively promoting the PANOPTESEC project in the context of H2020 consortiums and proposals to extend its results to the other connected security domains (e.g. Physical Security); and
6. Continued dissemination and informal presentations to selected stakeholders.

Complete details of the above activities are provided in the D8.1.4 Exploitation Report.

5.5 PANOPTESEC exploitation for academic partners

5.5.1 PANOPTESEC Exploitation by Institut Mines-Telecom

5.5.1.1 Partner profile and background

This Institut Mines-Télécom is a group of prestigious French engineering schools operating under the aegis of the French Ministry of Industry. It is focusing on the domains of Energy and Information and Telecommunication Technologies, and their applications (e-health, smart cities, green society, cyber-security, etc.). The Institute has 3 main missions:

- Higher education: the institute trains about 13000 students in its 15 schools, including around 9000 engineers (M level) and 1800 PhDs.
- Research and innovation: the Institute leads a strong research activity, with about 1700 ranked publications per year, 450 PhD defences and around 50 patents granted each year.

- Economic development: The institute contributes to about 100 start-ups founded by students or teaching staff, of which 85% are 3 years old or more

Institute Mines-Télécom is thus an active contributor to many of the French “poles de compétitivité” and “Instituts de Recherche Technologique” (IRT) that create networking opportunities and support for business creation and development.

5.5.1.2 Exploitation results and strategy

As an academic publication, IMT will of course participate in the dissemination of scientific knowledge through publications in conferences and journals, in the information security domain. Our policy is to publish few but solid papers, which can leverage interest in the security community.

Within the framework of PANOPTESEC, IMT is leading and developing an activity related to cyber-attack mitigation. This activity has matured up to the point that IMT has obtained recently a patent on the topic. We will continue to enhance our research to the point where we should be able to ask for more patents on the same topic, as well as be able to demonstrate our technology on use case scenarios to our industry partners. IMT actively seeks to transfer patents to industry, in order to foster development and commercial exploitation.

5.5.1.3 Risks and mitigation strategy

The main risk envisioned is that we are not successful in acquiring first, and transferring second, the patents that we wish to seek. This may lead to the decision to push some of these patents and the associated software into the public domain, if the cost of maintaining them becomes prohibitive for the Institute.

5.5.1.4 Implementation strategy

The implementation of our exploitation strategy will be twofold:

- Technology fairs: every year, IMT participates to or organises several technology fairs, either with small businesses or major partners. During these fairs, technologies are presented to interested industry partners in private meetings, and technology transfers are planned.
- “Challenge projet d’entreprendre”: every year in March, the school (Télécom SudParis) organises for its students an entrepreneurship challenge, where teams of students analyze a technology, the market, and create business plans. Proposals compete and the prize winners often develop their startup based on the challenge results. Our strategy is to propose this activity to a group of students interested in the domain of ICT security.

5.5.2 PANOPTESEC Exploitation by Universität zu Lübeck (UzL)

5.5.2.1 Partner profile and background

In 1973, the Universität zu Lübeck (UzL) became an independent scientific institution in the German state of Schleswig-Holstein. UzL offers degree programs in medicine, computer science, engineering, and natural sciences. Interdisciplinary programs encompassing natural sciences, computer science, and medicine offer practical and up-to-date education

underpinned by the highest standard in healthcare research. Compared with other universities, the Universität zu Lübeck is small, with just 3,400 students -- but has a good teacher-student ratio. The high standings of our computer science and medicine students point out the high standard of our teaching and education. In addition, Universität zu Lübeck intensively support technology transfer activities to support existing companies as well as new spin-offs. The University functions virtually as an incubator for the emergence of business concepts. The numbers of such University spin-offs have increased considerably in past years and have contributed essentially to the creation of new, highly-qualified workplaces. For this reason, spin-offs are particularly supported by special programs of federal and state authorities. In this frame, the Federal Ministry for Economy and Technology's promotion program EXIST plays a decisive role.

5.5.2.2 Exploitation results and strategy

As university partner within the PANOPTESEC consortium, UzL exploits PANOPTESEC results for scientific developments and foundational entrepreneurial activities. Fundamental research on theory related to the MIM has been published on major conferences. Further, theory on data collection and correlation as well as mission impact assessment have been published, and demonstrations of application scenarios were given for participants in applied workshops as well as for industry partners and contacts.

5.5.2.3 Risks and mitigation strategy

The main risk envisioned for UzL exploitation of PANOPTESEC is that the scientific results obtained are too specific, i.e., are too much tailored to the ACEA use case, and therefore do not transfer directly to other problem domains, such that PANOPTESEC gets wide acceptance in the academic domain. In the publications also other application areas have been investigated such that a wide application of PANOPTESEC results can be guaranteed.

5.5.2.4 Implementation strategy

The implementation of our exploitation strategy includes the following:

1. Publications: Scientific papers submitted to workshops, conferences and journals.
2. Technology demonstration events: UzL participates in industry conferences and demonstrations in relevant market segments, and shows demonstrators indicating the overall applicability and relevance of the problem solutions developed in research projects.

Further, the UzL has progressed towards direct exploitation using industry contacts and demonstrations. This includes, for example industrial contact with CYPP (cypp.de). CYPP is a small company and about to develop a data collection and security assessment software for medium-sized enterprises. They were very much interested in PANOPTESEC in general and the Data Collection and Correlation System in particular. A complete description of this exploitation opportunity is presented in the D8.1.4 Exploitation Report.

5.5.3 PANOPTESEC Exploitation by CentraleSupélec

5.5.3.1 Partner profile and background

CentraleSupélec is a prestigious French engineering school operating under the aegis of the French Ministry of Education and the French Ministry of Industry and ranked as one of the top in its fields. It is currently organized in a four campuses network located in Châtenay-Malabry, Gif-sur-Yvette, Rennes and Metz. It is focusing on complex systems engineering in the domains of energy, electronics, mechanics, aeronautics, space and information systems. 1000 engineering students (Master of Engineering level) graduate each year. CentraleSupélec also has a strong research activity with 300 research professors and 500 Ph.D. students. It is a member of the Pôle d'Excellence Cyber that regroups renowned French industries and academic partners working in cyber-defense.

5.5.3.2 Exploitation results and strategy

As an academic partner, CentraleSupélec will participate in the dissemination of scientific knowledge through publications in conferences and journals, in the information security domain. Our policy is to publish solid papers in international conferences and to participate to technical conferences, workshops and technology fairs, which can leverage interest in the security community.

Within the framework of PANOPTESEC, CentraleSupélec is participating in the activities of data collection, intrusion detection and visualization. The first objective of CentraleSupélec is first to integrate its expertise in these three domains in a complete integrated solution. Then, thanks to experiences performed with this solution on real cases, it will be possible to identify the theoretical limits and practical issues and to improve each component as well as their integration. The second objective of CentraleSupélec is then to be able to provide software components that can be profitably easily integrated to numerous security systems.

5.5.3.3 Risks and mitigation strategy

The main risks envisioned for CentraleSupélec exploitation of PANOPTESEC is that the scientific and technical achievements of the project do not meet objectives to experiment and validate the resulting solution on a sufficiently significant use case to demonstrate the relevance of the components and of their integration. The mitigation strategy for CentraleSupélec is to use accurate, precise and as standard as possible interfaces to its components to be able to interact with existing technologies. If no standard is available, the data model used in the components should allow easy transformation of the existing data formats.

5.5.3.4 Implementation strategy

The implementation of our exploitation strategy will be made of three parts:

- Participation in international conferences and workshops to leverage interest of the security community.
- Presentation of the PANOPTESEC project and of its results to the partners of the French Pôle d'Excellence Cyber.

- Participation to technology fairs: every year, CentraleSupélec and INRIA participate to several technology fairs. For instance, CentraleSupélec and INRIA were very active this year in FIC (Forum International de la Cybersécurite) in Lille where it presented results in visualization for cyber-security.

5.5.4 PANOPTESEC Exploitation by CIS-UROME

5.5.4.1 Partner profile and background

UROME unit is made by two main subgroups: distributed and dependable systems group and information visualization group. Both the sub-groups are internationally recognized by their respective communities and have several collaborations with national companies (e.g., IBM, Microsoft) and public administrations and agencies (e.g. Italian national security agency, Minister of the Finance). Recently, most of our efforts have been devoted in the analysis and design of dependable architecture in the Context of Critical Infrastructure protection.

As part of a Research Centre attached to Sapienza University, we have two main missions:

- Higher education: people involved in the CIS are members of Sapienza University of Rome, the main and ancient University of the city that trains thousands of students each year.
- Research and innovation: the research centre has a strong and sustained research activity, witnessed by the high publication rate in high-level peer-reviewed international journals and conferences.

5.5.4.2 Exploitation results and strategy

From a strategical perspective, being an academic partner, the main exploitation activity of UROME will be devoted to the merger of PANOPTESEC results into its usual communication policy, through articles published in professional and technical press and scientific journals, communications and presentations at research and business conferences (including the IST conferences organized by the EC), trade shows and professional exhibitions.

Furthermore, the use of the results and their publication not only in Italy but also within countries of the European Union will be guaranteed by the institution's large network in the public and private sector.

UROME will exploit its results using its contact network built through several past projects with Public Administrations trough and its experience in developing applied research. This will be also favored by its geographic location (established in Rome, where the Italian Government institutions are also established, and the Italian National Centre for IT in the Public Administration). As a consequence, we expect a high impact of the dissemination of the project results towards the most interested users, especially among public administrations and big companies ready to invest in the cyber defense.

As potential publication venue, UROME is specifically interested in journals, conferences and workshops related to Database, Distributed Systems, Service-oriented Computing, Mobile Computing and Information Visualization.

Given the two assets (Visualization Environment and Query-based High-Level On-line correlation engine, namely QBE) that CIS-UROME established with PANOPTESEC, some exploitation activities have been already carried out and described in the following:

- CIS-UROME transferred basic concepts behind PANOPTESEC into specialized lectures offered to students attending specialized courses of the Master in Engineering in Computer Science offered by the School (e.g. course of Seminars in Distributed Systems and Information Visualization).
- CIS-UREOM are setting up a research collaboration with the Academic Centre of Excellence in Cyber Security Research at Imperial College London (Prof. Emil C. Lupu and its group) to further develop and extend the functionalities of QBE.
- Following the successful experience with the spin-off Over Technologies (following from a previous FP7 project), CIS-UROME are investigating the feasibility of a new spin-off.

5.5.4.3 Risks and mitigation strategy

CIS-UROME do not envision particular risks in the fulfillment of our exploitation plan.

5.5.4.4 Implementation strategy

Due to the CIS-UROME nature of Academic body, the implementation of our exploitation plan falls within the normal institutional duties and common work.

6 CONCLUSIONS

6.1 Significant results achieved

In this document, a summary of the dissemination and exploitation activities, strategies and plans are presented, with reference to outcomes already achieved. It is not intended that this document provide extensive details of dissemination and exploitation activities since these results are otherwise presented in the D8.1.3 Dissemination and D8.1.4 Exploitation Reports.

In this document, the foundation for the dissemination activities has been set, including the development and maintenance of the website and the overall project branding and logo as well as the production of this report which summarises the activities roadmap that have been followed to ensure the optimal dissemination and exploitation of PANOPTESEC results.

The project developments have been regularly disseminated through the website, social media presence, and a significant number of various publications (conferences, papers, posters, lectures etc.).

In addition to the dissemination activities based on the DoW, additional workshops have been identified and have been executed to present the perceived cyber-security challenges in the cloud environment, to conduct demonstrations of some PANOPTESEC prototype capabilities, and to obtain feedback from providers and the market players concerning the project. These activities have also provided a great visibility for the project to relevant stakeholders. This is particularly true of the final operational workshops spanning the period 17-28/10/2016.

During this period a significant result was the elaboration of detailed Exploitation Plans per partner which have been added to this report and with reference to more detailed information available in the D8.1.4 Exploitation Report. The PANOPTESEC project aims to follow a broad academic and commercial distribution strategy, which will build on the beyond-state-of-the-art technologies that will be developed during the project lifetime. The PANOPTESEC consortium exploitation plan represents the collective intent of the consortium to pursue the results of the project to the maximum extent possible.