FP7-SEC-2011-1 Project 285647

Cybersecurity on SCADA: risk prediction, analysis and reaction tools for Critical Infrastructures

D7.1 - Dissemination and exploitation plan-Final

General information	
Submission date	07/04/2015
Dissemination level	Public
State	Final version
Work package	WP7000 – Dissemination & Exploitation
Task	Tasks 7001 - 7002
Delivery date	31/12/2014

Editors

Name	Organisation
M. Aubigny, A. Mckinnon, M. Martins, C. Harpes	itrust consulting

Authors

Name	Organisation
M. Aubigny, A. Mckinnon, M. Martins	itrust consulting

Reviewers

Name	Organisation	Date
Paulo Simoes	University of Coimbra	01/04/2015
Stefano Panzieri	Roma3	01/04/2015

Table of contents

List of figures

List of tables

1 Introduction

1.1 Context

Several different methods of dissemination and exploitation will be used in order to promote the results of the CockpitCI project.

1.2 Objective

The objective of this document is to provide an overview of the dissemination and exploitation activities related to the CockpitCI project. All the activities aim to provide external visibility to the project's results and will include scientific, technical, commercial and industrial points of view. For the major milestones of the project the consortium will publish a press release.

1.3 Document Structure

This document is structured as follows:

- Chapter 2 presents the CockpitCI informational website;
- Chapter 3 describes the planned demonstration of the concepts developed during the project;
- Chapter 4 provides details of the conferences that project partners will attend and/or contribute to;
- Chapter 5 outlines the publication, seminar and conference dissemination strategy.
- Chapter 6 presents the exploitation plan of the project during the project and for the future

1.4 References

1. DOW_CockpitCI_(285647).pdf
2. CockpitCI-D7.1.1- Dissemination and Exploitation-Preliminary-1.pdf, November 2012
3. CockpitCI-D7.1.2- Dissemination and exploitation plan-Intermediate-1.pdf, November 2013

1.5 Glossary

Terminology	Description
WP	Work Package

1.6 Acronyms and symbols

Acronym or symbols	Explanation
CockpitCI	**C**ybersecurity **o**n S**C**ADA: ris**k** **p**rediction, analysis and reaction **t**ools for **C**ritical **I**nfrastructures

2 CockpitCI website

2.1 Introduction

The website contains both public and restricted parts. With regards to dissemination, only the public part of the website is relevant and includes the project presentation and a blog.

The project presentation includes a general description of the project and partner profiles. The project achievements will be posted here as and when they are realised.

A blog hasl also be used to enhance interactivity amongst the community and may also be used for receiving comments or suggestions.

The main address of the website is: www.CockpitCI.eu. The website is managed and hosted by itrust consulting.

During the project and in relationship with the dissemination action lead by the consortium, a re-design of the web-site has been envisaged and implemented especially in line with the exhibition of the project result at Brussels for the 2014 Cigre Congress. The main objectives were to enhance the visibility of the project and increase the number of visits to the web-site.

2.2 Version 1 of the CockpitCI web site

2.2.1 Web-site V1 architecture overview

Figure 1 shows the website architecture:

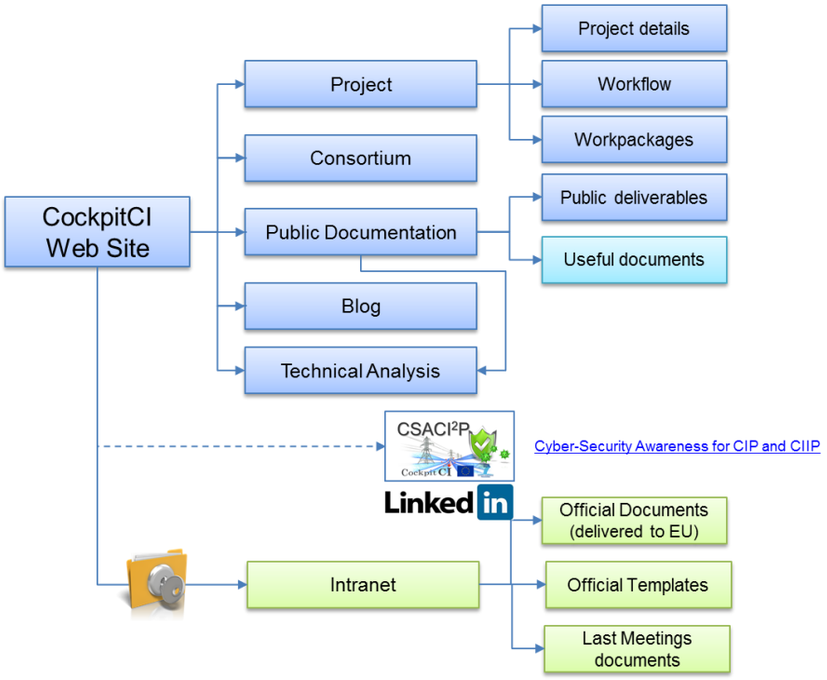


Figure 1: Website V1 architecture

The public area of the website (blue boxes cf. Figure 1) provides information on the project as well as SCADA security research. The private area (green boxes cf. Figure 1) is reserved for the consortium members to upload useful documents such as project deliverables. The deliverables (unless they are authorised as public by the reviewers of the commission) are not available in the public area.

The security of the website is continuously monitored by itrust's Consulting and Hacking Department in order to avoid security breaches.

2.2.2 Presentation of the project

The first aim of the website is to provide visitors with a general overview of the project.

2.2.2.1 Overview of the project

The homepage of the web-site describes the objectives, work description, and expected results of the project. Specific pages in the "Project Tab" summarise the main expectancies of the project and present the general management in terms of work packages and work-flow.

Figure 2: www.CockpiCI.eu homepage

Figure 3: Project Summary

The project details description provides information on the technical and standardisation issues relating to the project.

The web-site describes each of the individual work packages and the relationship between them (cf. Figure 4).

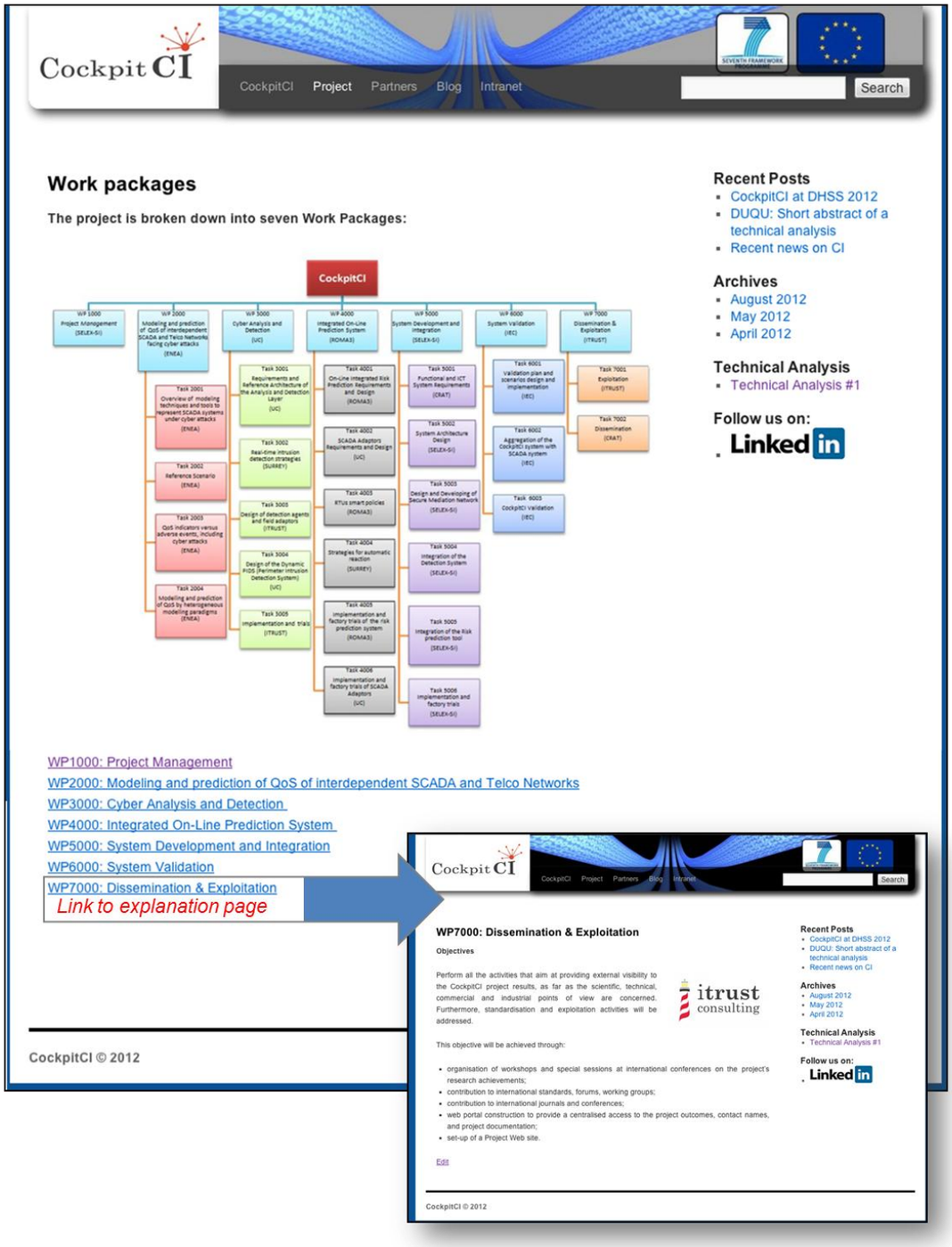


Figure 4: Structure of the project

On the partners' page, a brief description of every member of the CockpitCI consortium is provided as well as a link to each of their websites:

Figure 5: Description of partnership

2.2.2.2 Specific dissemination web-pages

In order to provide good exposure to the project, the website contains CockpitCI public deliverables, general documentation on project topics (e.g. European Critical Infrastructure Protection Strategies, technical studies on CIP and cybersecurity), and advertisement materials designed during the project.

Figure 6: Documentation provided through the web-site

Furthermore, the website also contains a blog in order to initiate discussions on cyber-security topics applied to Critical Infrastructures and obtain comments and feedback from stakeholders, software manufacturers, end-users, and implementers.

Each partner should submit a paper or provide feedback in order to keep the site current and up to date. Every two months we should have a new document which reflects the technical progress of the project or provides an analysis or abstract on the current state of Critical Infrastructure security and the latest threats.

Figure 7: First blogposts in the CockpitCI web-site

To improve the dissemination of the project and the interaction between stakeholders, a professional group has been set up on the social network LinkedIn. The name of this group is CSACI²P: Cyber-Security Awareness for CIP and CIIP. Currently, the group is not "open" in order to base its foundations on the specific relationship of project partners with manufacturers, groups of specialists or potential users of the CockpitCI System. The first discussion, as shown in the abstract below, has been intentionally based on a polemic security topic i.e. the manufacturer strategy of security mainly based on technical obfuscation of their products.

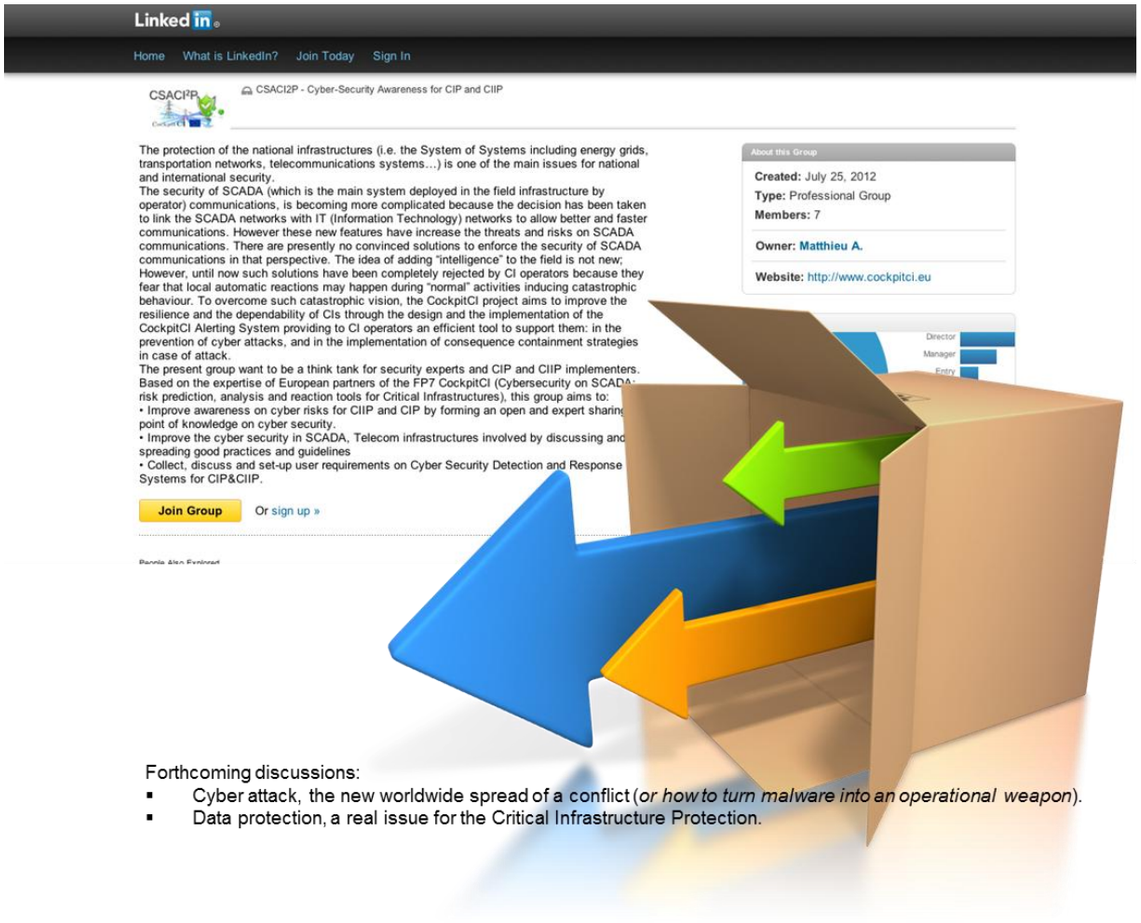


Figure 8: LinkedIn Group of CockpitCI: CSACI²P

To improve the use of the LinkedIn group and increase the project dissemination, the forthcoming discussion of the group will be to focus first on the strategic issues of both the cyber-attacks of Critical Infrastructures (in the art of the 21st century war) and cyber security and secondly on the new Data protection challenges related to the deployment of smart meters in the management of Critical Infrastructures. The definition of new topics of discussion should be defined every quarter by partners and supported by spreading information.

The website has been officially published in June 2012 and was informally presented to stakeholders during the Luxembourg Grand Ducal visit to Berlin in June 2012, during the DHSS 2012 conference and during the Romanian conference in October through the distribution of CockpitCI flyers (cf. Chapter 8).

The website also provides a dedicated page providing technical analysis on topics such as:

- Malware or exploit of technical products (hardware, software or firmware) deployed in the field.
- Tactical and operational counter-measures set-up during the project and establishment of new good practices in security management of CIP and CIIP.
- Strategic issues of security management especially in terms of operational cooperation between the several teams involved in the global security of Critical Infrastructures (Security Incident Response team, SCADA team, ICT team and top management).

2.3 Version 2 of the CockpitCI web site

The new version of the web-site has been launched on March 2014 and will be maintained after the end of the project to facilitate the exploitation of the projects results.

2.3.1 Web –site V2 architecture overview

The main improvement of the version 2 of the web-site was based on a new design to provide a more friendly approach of the project and to provide a sustainable platform on project results and exploitation overview. In that aim, the architecture of the web-site has been simplified as described in the following figure:

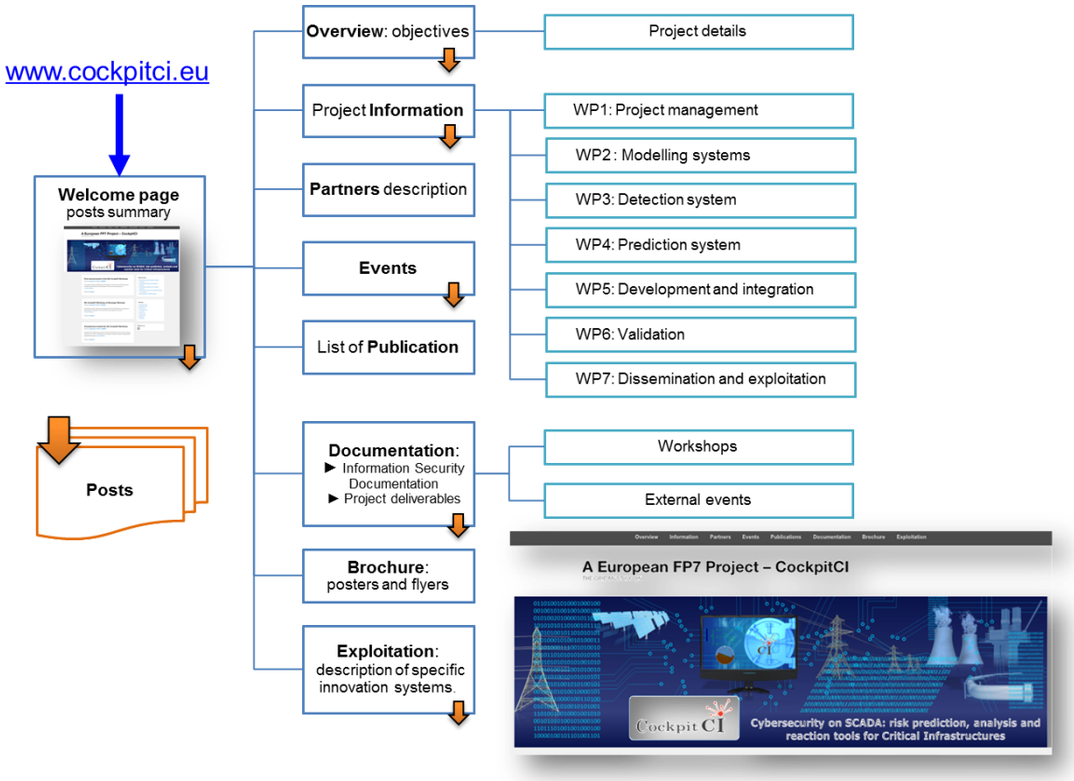


Figure 9: Website V2 architecture

2.3.2 Design and content improvement

As already mentioned, the main improvement of the web site has focused on the design of the web site in relationship with the consortium decision to participate to the Cigre Congress 2014 as exhibitor. The web-site should be based on the same type of layout that the exhibition material produced for the Congress exhibition. The visual aspect of the web page has been improved to underline the innovation and wide application area of the systems developed during the project.

Figure 10: New design of web-site V2

The content of the web-site has been updated and improved monthly according to the project progress e.g. reporting of workshop, events or new publication of partners. All relevant events as workshops has been reported trough a dedicated posts and some posts have been write to disseminate relevant information on CIP and CIIP: such as information about Stuxnet analysis or cyber-attack on Critical Infrastructure.

3 Demonstrations

We intend to perform at least two major demonstrations during the last six months of the project: the first being either in Israel, Norway or Romania to show the efficiency of the system for the partners' top management. The second demonstration would be located in Europe, either in Brussels or Luxembourg in order to debrief the results to Commissioners and to present the system to potential European end-users and stakeholders. The main goal of these demonstrations will be to receive manufacturers', end-users' and stakeholders' feedback and be able to foresee a real deployment of the solution, including its fine-tuning and embodiment in a software/hardware package. These two main demonstrations will be preceded by small display events of the system, organised during project workshops according to the current progress.

3.1 Demonstration strategy

The demonstration of the solution in a real environment has four main goals:

1. To validate the technology of the solution in a controlled environment less restrictive than a laboratory environment.
2. To disseminate the technical issues to the scientific community (especially the standardisation issues). This goal shall be linked with the consortium's effort to submit scientific papers.
3. To disseminate the solution to manufacturers, stakeholders and end-users especially in European security agencies and professional groups of Critical Infrastructure owners.
4. To present the results to the European Commissioners and others stakeholders.

The objective is to have a process that collects feedback from the demonstrations to improve the prototype in order to reach end-user needs. The scheme below describes the feedback improvement cycle included in this strategy. It has been based on the PDCA improvement cycle.

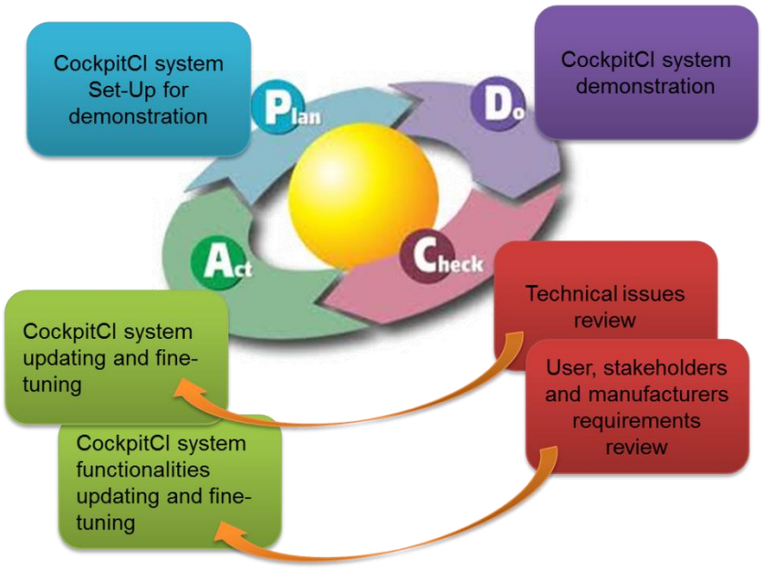


Figure 11: Exploitation of CockpitCI demonstration results

3.2 Tactical framework of the demonstrations

As IEC will provide remote access to the virtual test-bench deployed for the project and simulating the power-grid, telecommunication and operation networks' behaviour, and others partners (Roma3, FCTUC, itrust) have designed or intend to set up their own sand boxes to test the CockpitCI system, each demonstration event could include different levels of demonstration linked to whole set of sub-systems deployed into the CockpitCI system and linked to the tactical level of response of the CockpitCI system (Detection, Analysis and Response levels).

1. Limited demonstration of detection, analysis and response tools based on historical databases of incidents, attack scenarios or samples. This also includes a demonstration of specific algorithm of detection or response set up by some specific partners.
2. Global demonstration of the system including the remote access to sand-boxes or test benches deployed in partner's laboratories to test the interdependency aspect of the system and the real-time functionalities.

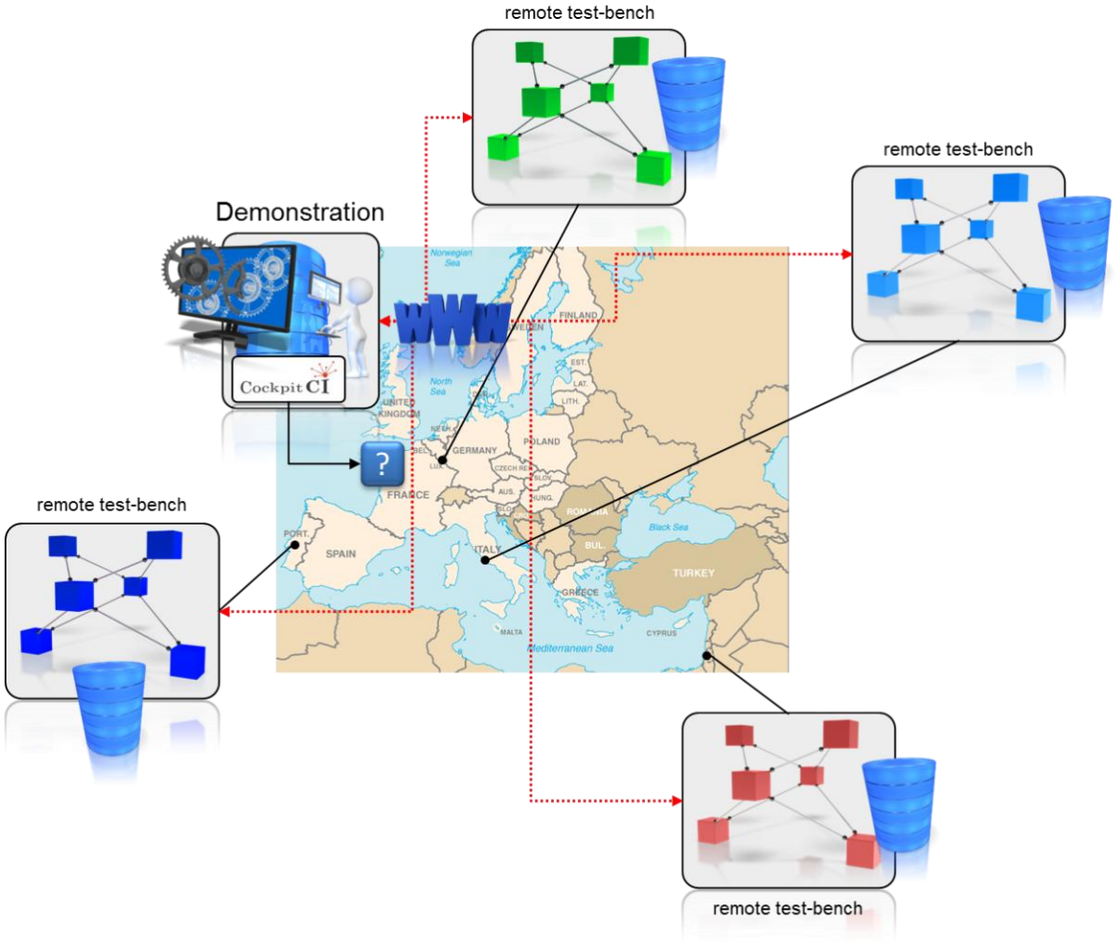


Figure 12: Tactical framework of the demonstrations

3.3 Reporting of demonstration events

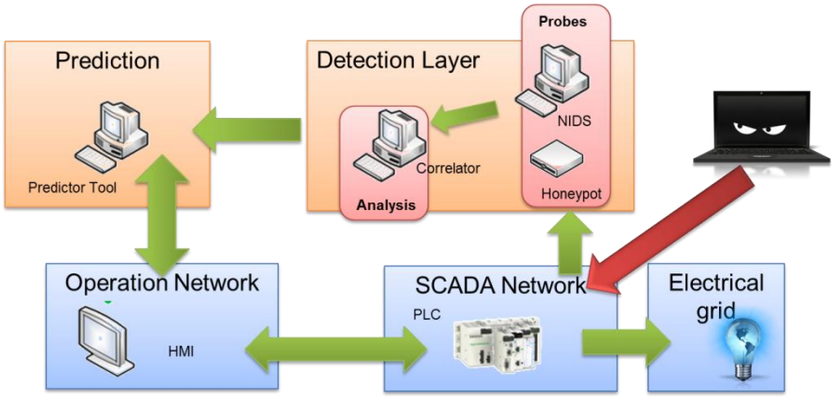
According to the Do Work of the project, the CockpitCI consortium have organised several demonstration of the CockpiCI system for potential stakeholders. These exhibitions have taken place either during specific even or during workshop organised by partners in their facilities.

3.3.1 Demonstration at Cigre Congress (Brussel)

The main demonstration in terms of total amount of visitors has taken place during the Cigre Congress in Brussels on 12th to 14th March. This international event, titled "*Innovation for Secure and Efficient Transmission Grid*", organised by the AIM (Association des Ingénieurs de Montefiore) has met together the main actors of SCADA deployment in terms of efficiency and security and international stakeholders coming from all over Europe but also from South America or Asia. During these two days, more than 650 people have the opportunity to become aware of the project (a dedicated flyer have been distributed into the Congress bag) and to participate to a demonstration of some major components of CockpitCI system (Risk Prediction Tools and Detection tools) at the CockpitCI Stand. The demonstration was performed by members of the Universities of Coïmbra and Roma 3 and supported by itrust consulting, especially for logistic aspects.

Figure 13: Cigre Congress – CockpitCI stand

As the connection with IEC test bed was not ensured, the demonstration was based on a small physic test bed composed by a simple PLC connected to a relay controlled a light. Several types of attacks on this PLC and on the monitoring system of this PLC (HMI) were performed to make aware visitor on the risk of cyber-attack and on the need of specific detection components like the components developed in the project. The attacks performed were the following: network scan attack, flooding attacks and man in the middle attacks on PLC network. According to the detection layer, the CopckpitCI prediction tool was able to compute the potential effect of the attack on a virtual environment including telecommunication, SCADA networks (targeted PLC included), and electrical grid. This tool allowed assessing the risk to use the targeted PLC during a process of re-energizing of the grid (FSIR scenario) after an incident (e.g. impact of the lightning on a node of the electrical grid).



This demonstration allowed not only measuring the interest of the main stakeholders on the detection but also assessing the awareness level of them on cyber-attacks on the control network of the electrical grid. Even if the eventuality of a cyber-attack is not ignored, the awareness level of the main actors (providers of electrical grid control system or users of such systems) seemed to remain low in regards to the real threat on these operational systems.

3.3.2 Demonstration at ENEA Headquarter (Roma)

The demonstration at the end of the project during the Roma Workshop on 16th December 2014 allowed demonstrating for the first time an integrated system of the main Cockpit solution components: i.e. the test bed located in IEC premises, detection system and prediction system working together under several types of cyber-attacks not only on SCADA network (MITM attack) but also on telecommunication network (Dos attack on switch).

The event allowed demonstrating:

- The visualization of FISR scenarios on test bed in normal state and under attacks.
- The detection networks functioning: network NIDS/HIDS, Field NIDS, SCADA Honeypot, and Shadow RTU, local and main correlators.
- The dedicated system of attack management allowing testing the CockpitCI system with different types of attacks.
- New Risk Prediction tools (CISIA).

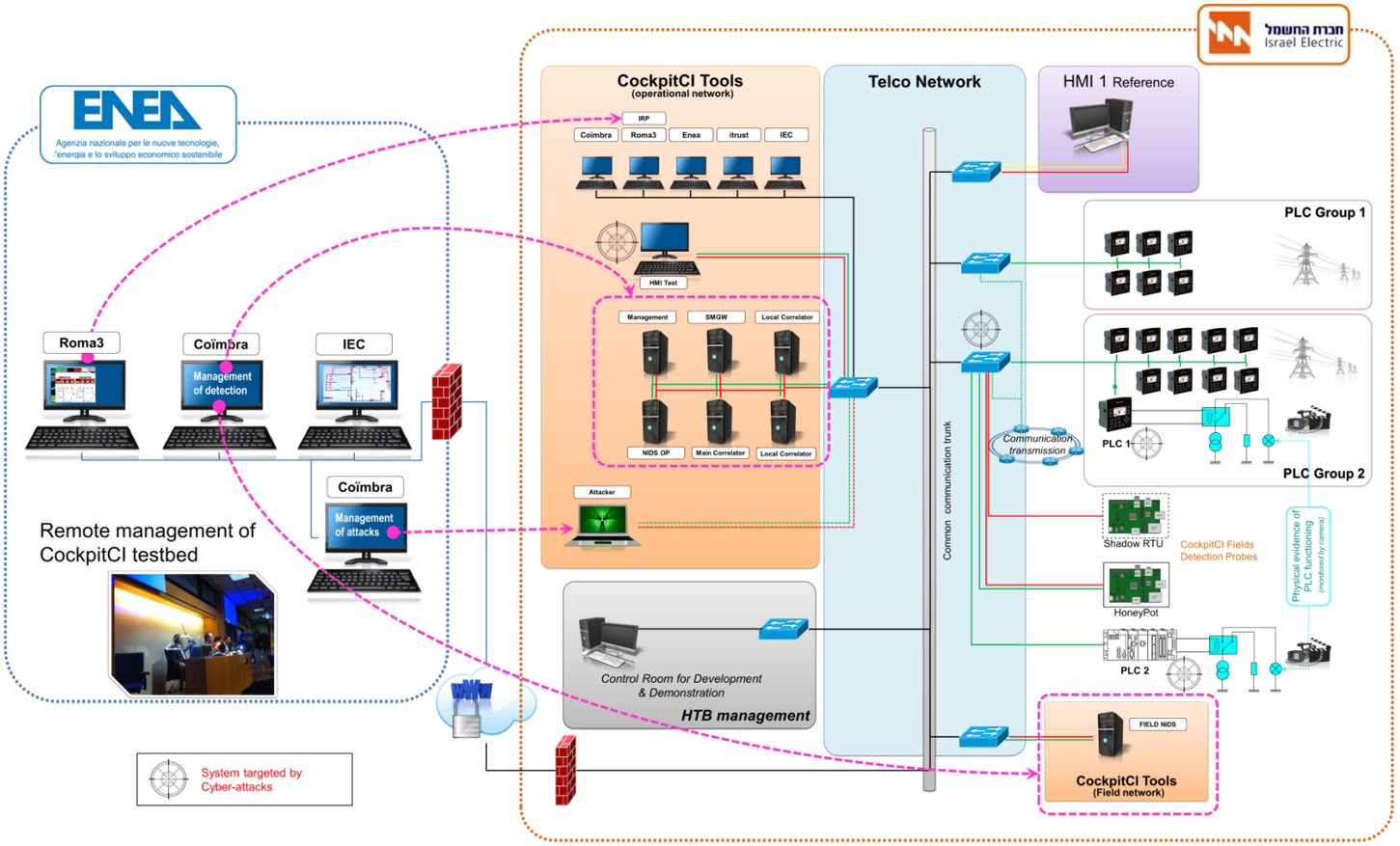
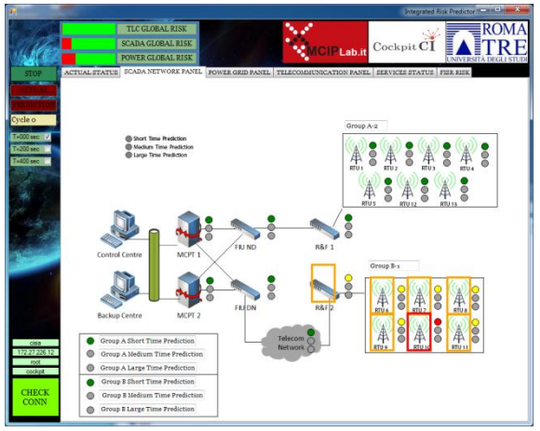


Figure 14: Demonstration of CockpitCI system at Roma Workshop 2014

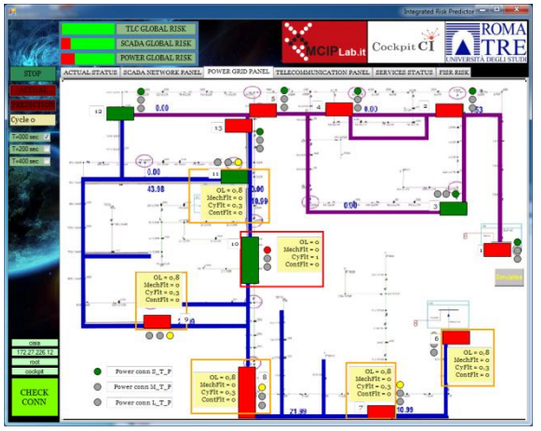
As shows the figure above, the all the demonstration was remotely controlled from ENEA premises trough a VPN connection to IEC test environment. The demonstration progress has been set up into three phases:

3. Demonstration of the electrical grid simulation environment especially the behaviour of the electrical grid in case of malfunctioning and during FSIR scenarios.
4. Simulation of attacks performed by operator managing a dedicated virtual machine located into IEC environment (it was an assumption of the demonstration).
5. Visualisation of the detection results (IDMEF message describing the security incident) into the Risk Prediction Interface for the three monitored networks (scada, electrical grid and telecommunication network).
6. Simulation of the FISR scenarios into the RPT to assess the risk of re-energizing process using such FSIR scenarios in case of cyber-attacks.

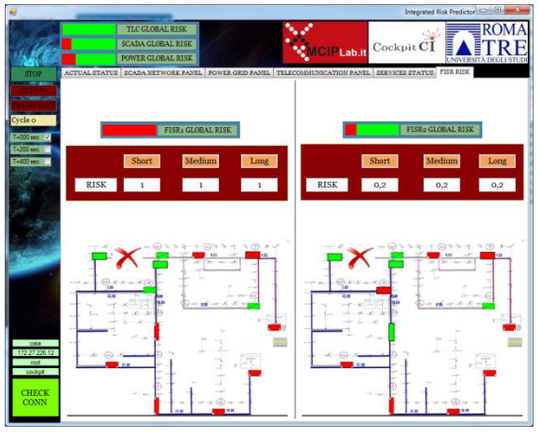
The figures below show the RPT monitoring interfaces allowing to the electrical grid operator to have more information about the risk level of the infrastructure and a specific assessment of the defined FSIR scenarios.



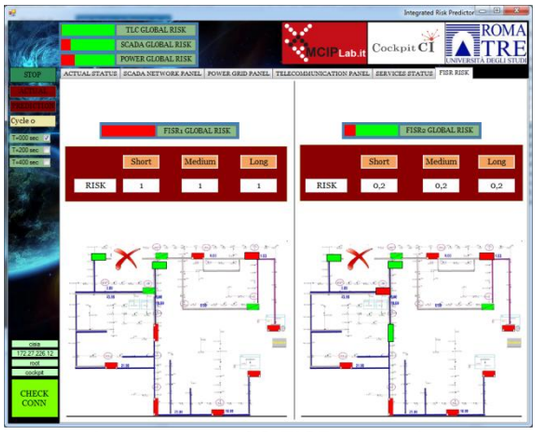
Behaviour of the telecommunication network during a flood attacks



Behaviour of the electrical grid during a flood attack



Assessemnt of 2 FISR scenarios in case of a flood attack



Assessment of 2 FISR scenarios in case of scan attack.

3.3.3 Other demonstrations

On the occasion of workshops of Luxembourg, Bucharest and Stavanger (cf. description below), additional demonstration of other tools, developed during the project, has been provided by the consortium. The table below gives a quick overview of the demonstrations performed by partners.

CockpitCI Tools	Luxembourg	Bucharest	Stavanger	Roma	Partner	Type of demo
Virus spreading models	✓	✓	✓	✓	ENEA	PowerPoint presentation of the model and video examples of the model functioning
QoS RAO Modelling		✓	✓	✓	Multitel	PowerPoint presentation of the model tool and (in the last two workshops) demonstration in life of the tools on test samples.
Meta-Antivirus AV Caesar	✓	✓		✓	itrust	PowerPoint presentation of the tool, live demonstration or video of the tool functioning.
Software Vulnerability Checker	✓	✓		✓	itrust	PowerPoint presentation of the tool, live demonstration or video of the tool functioning.
OCSVM: Integrated detection mechanism	✓	✓		✓	Surrey	PowerPoint presentation of the tool with results of real samples
Smart RTU		✓	✓	✓	Roma3	PowerPoint presentation of the tool.
Shadow RTU				✓	FTCUC	PowerPoint presentation of the tool

Table 1: List of short demonstration of specific CockpitCI tools

4 Workshops

This section will provide a description of the workshop performed during the CockpitCI project. The section will describe the purpose and include the list of conferences, discussion and the material used to disseminate the CockpitCI idea. The section will also include the main findings for the project (if possible)

4.1 Workshop in Israel (IEC and itrust)

On the 14th December 2012, the project team organised a workshop that brought together about one hundred cybersecurity specialists. The objective of the workshop was to have an open confrontation on the issues addressed by the CockpitCI project with End Users and System Manufacturers in the Energy, ICT and Control Systems sectors. The project team had the opportunity to collect feedback via a questionnaire that was distributed to the audience.

4.1.1 Organisation

The objective of the workshop was to have an open confrontation on the issues addressed by the CockpitCI project with End Users and System Manufacturers in the Energy, ICT and Control Systems sectors.

4.1.2 List of presentations

Topic	Presenter
Building Your Security Strategy in a Vulnerable World	A. Bar Lev, Check Point President, Israel
SCADA Systems Cyber Security Challenges of European Utilities	A. Kvinnesland, Lyse IT Security Advisor, Norway
CockpitCI: Project overview	SELEX-SI, Italy
Modelling Industrial Control Systems under cyber-attacks	ENEA, Italy
The problem of detecting cyber-attacks in SCADA systems	University of Coimbra, Portugal
Cyber-physical risk prediction	Roma3, Italy
Hybrid test bed for Industrial Control Systems of Critical Infrastructures	IEC, Israel
Dissemination and exploitation	itrust consulting, Luxembourg

4.1.3 Findings

The workshop put together many players from Israeli industry linked to the electric sector. An important delegation from IEC provided field expertise to research partners.

A questionnaire was distributed to collect feedback from the audience.

4.2 Workshop in Portugal (FTCUC and itrust)

The objective of the workshop was to have an open discussion on the issues addressed by the CockpitCI project with End Users and System Manufacturers in the Energy, ICT and Control Systems sectors. In the first part of the workshop, the CockpitCI concept was presented. In the second part, selected presentations from industry stakeholders provided an overview of current industry needs and practices. The workshop finished with a joint discussion panel.

4.2.1 Organisation

The 2nd CockpitCI Workshop took place in Coimbra, Portugal, in March 20th 2013. It was hosted and organized by University of Coimbra, with the support of other CockpitCI partners.

Its half-day program – included in Annex A – included a set of technical presentations about the CockpitCI Project and a set of presentations from invited Portuguese industry speakers. More specifically, the following external speakers were invited to participate:

- ***Cybersecurity in Electricity Distribution***, by Nuno Pereira (EDP)

EDP (http://www.edp.pt/) is the largest Portuguese energy utility, with operations in a wide number of countries (Asia, Southern Africa, Europe, Southern America, North America), including electricity and gas distribution and electricity production (renewable and fossil sources). This talk focused on the needs and future strategy of EDP, regarding cyber security for distribution grids, from an operations point of view. Related research projects with the participation of EDP were also addressed.

- ***FeedZai Pulse: Uncover and Manage Anomalies in Real-Time***, Paulo Marques (FeedZai)

FeedZai (http://feedzai.com/) is an SME specialised in real-time business intelligence platforms. Its Pulse platform has been successfully deployed in a wide range of application fields, including online credit card fraud detection, online processing of monitoring data provided by large wind farms (production forecast) and online processing of SCADA events produced by HV/MV distribution grids (with reference scenarios of around 400 substations). This presentation provided an insight on how to analyse large data sets in real-time, and on how this could be applied to cyber security in industrial control networks.

- ***CECRIS – CErtification of CRItical Systems***, by Marco Vieira (University of Coimbra)

This presentation provided an insight on CECRIS, a European project focused on the improvement of verification, validation and certification of critical systems (http://www.cecris-project.eu/). Possible liaison points between CockpitCI and CECRIS have been discussed.

- ***Energy Metering***, by Nuno Martins (ISA – Intelligent Sensing Anywhere)

ISA (www.isa.pt) is a leading SME in the fields of remote telemetry, namely in the fields of electricity (sub-metering platforms), oil and gas distribution. In this presentation, Nuno Martins addressed the security requirements and solutions deployed on the various types of sensors developed by ISA, as well as on the impact of smart grids on cyber security.

Some photos of the Workshop are available on the CockpitCI web-site.

4.2.2 List of overall presentations

Domain	Topic	Presenter	Organisation
The CockpitCI approach to Cyber Security - Moussa Ouedraogo, Public Research Center "Henri Tudor" ·	CockpitCI project overview	Antonio Graziano	SELEX
	Scenario and models of SCADA and ICS under cyber attacks	Michele Minichino	ENEA
	Smart detection strategy	Tiago Cruz	University of Coimbra
	Cyber-risk prediction strategy	Stefano Panzieri	Università di Roma Tre
Industry Perspectives – Miguel Martins, itrust consulting	Cyber security in electricity distribution	Nuno Pereira	EDP
	Uncover and manage anomalies in real-time	Paulo Marques	FeedZai

	CECRIS – CErtification of CRItical Systems	Marco Vieira	University of Coimbra
	Energy metering	Ricardo Clérigo	ISA
Panel Discussion	Towards safer critical infrastructures	Antonio Graziano, Marco Vieira, Michele Minichino, Nuno Pereira, Paulo Marques, Ricardo Clérigo, Stefano Panzieri, Tiago Cruz	

4.2.3 Findings

The workshop gathered more than 50 attendees (mainly from national industry, graduate students and researchers from Portuguese universities and national organisations) who actively participated in the discussions, providing valuable feedback to the CockpitCI Project and good networking and exploitation paths that will be explored in the future.

4.3 Workshop in Luxembourg (itrust consulting)

Organised under the patronage of the Ministry of Economy, the objective of the workshop was to present the first results of the CockpitCI project to Great Region (Luxembourg, border area of Belgium, France and Germany) End Users and System Manufacturers in the Energy, ICT and Control Systems sectors. In the first part of the workshop, the CockpitCI concept and first results were presented. In the second part, selected presentations from security regulation authorities (ENISA and Luxembourg Ministry), Luxembourg Electrical provider CREOS gave an overview of the main issue and difficulties to deploy sustainable CIP. The workshop finished with a joint discussion panel.

4.3.1 Organisation

The 3rd CockpitCI Workshop took place in Luxembourg City, Luxembourg, in March 10th 2014. It was hosted by CREOS and organized by itrust consulting, with the support of other CockpitCI partners.

Its half-day program – included in Annex A – included a set of technical presentations about the CockpitCI Project and a set of presentations from invited Luxembourg and European organisation speakers. More specifically, the following external speakers were invited to participate:

- ***Experience of SCADA upgrading project***, by Carlo Bartocci (CREOS)

CREOS (http://www.creos-net.lu) is member of the Group Enovos. Creos Luxembourg S.A is the owner and the administrator of networks of electricity and mains of natural gas in the Luxembourg. More than 650 people are in the service of the company today. The mission of Creos consists in operating in a not discriminatory way the energy market, so that all the current and potential suppliers have access, under identical conditions, to its networks of transport and supply of electricity and natural gas. In this context, the company is responsible for the planning, the realization, the maintenance and the high, average and low-voltage management of electricity networks and for the high, average and low-pressure natural gas management. Networks managed by Creos include approximately 9.000 km of electric lines and approximately natural 1.850 km of gas mains, as well as about 245.000 customers in electricity and about 45.000 customers were linked with the natural gas.

- ***Recent evolution of the CIP and CIIP for SCADA***, Konstantinos Moulinos (ENISA)

ENISA (https://www.enisa.europa.eu) agency's Mission is essential to achieve a high and effective level of Network and Information Security within the European Union. Together with the EU-institutions and the Member States, ENISA seeks to develop a culture of Network and Information Security for the benefit of citizens, consumers, business and public sector organisations in the European Union. ENISA is helping the European Commission, the Member States and the business community to address, respond and especially to prevent Network and Information Security problems. ENISA is as a body of expertise, set up by the EU to carry out very specific

technical, scientific tasks in the field of Information Security, working as a "European Agency". More specifically, ENISA's Critical Information Infrastructure Protection (CIIP) and Resilience Unit is responsible for assisting competent national EU agencies, private sector and EU Commission to develop sound and implementable preparedness, response and recovery strategies, policies and measures that fully meet the emerging threats critical information infrastructures face today.

- ***The Government as key stakeholder for CI Cybersecurity***, by Paul Rhein (HCPN)

The Haut Commissariat à la Protection Nationnale (HCPN) is a past of the State Ministry in Luxembourg in charge of Critical Infrastructure Protection. It works in partnership with the GovCERT (http://www.govcert.lu), also known as the computer security incident response team (CSIRT). GovCERT.LU is the single point of contact dedicated to the treatment of all computer related incidents jeopardising the information systems of the government and of critical infrastructure operators.

Some photos of the Workshop are available on the CockpitCI web-site.

4.3.2 List of overall presentations

Domain	Topic	Presenter	Organisation
The CockpitCI approach to Cyber Security	Introduction	Carlo Harpes	itrust consulting
	Overview of the CockpitCI Project	Antonio Graziano	SELEX
	The CockpitCI multi-layered detection framework	Paulo Simoes	FTCUC
	Modelling the loss of controllability and observability of electrical grids under SCADA cyber attacks	Michele Minichino	ENEA
	Risk Prediction Tool of CockpitCI system	Stefano Panzieri	Roma Tre
	Attributes extracted from network traces	Leandros Maglaras	Surrey University
	Presentation of specific CockpitCI tools	Matthieu Aubigny	itrust consulting
Industry and regulation perspectives	Recent evolution of the CIP and CIIP for SCADA	Adrian Pauna	ENISA (by skype)
	Experience of SCADA upgrading project	Carlo Bartocci	CREOS
	The Government as key stakeholder for CI Cybersecurity	Paul Rhein	Haut Commissariat à la Protection Nationale
Panel Discussion	Critical infrastructures protection	Carlo Harpes, Antonio Graziano,Carlo Bartocci, Michele Minichino, Stefano Panzieri, Paulo Simoes	

4.3.3 Findings

The workshop gathered around 20 attendees (as the workshop was located in the control centre of Creos, it could not welcome lot of people) who actively participated in the discussions, providing valuable feedback to the CockpitCI Project and good networking and exploitation paths that will be explored in the future. The presentation of ENISA and CREOS were very useful to assess the real need of security system for the future.

4.4 Workshop in Bucharest (Transelectrica)

The objective of the workshop was to present the main results of the CockpitCI project to End Users and System Manufacturers in the Energy, ICT and Control Systems sector and collect their needs in terms of security. The

workshop has been focused on the presentation of the CockpitCI concept and on the main results of the project. The workshop will finish with a joint discussion panel.

4.4.1 Organisation

The 4th CockpitCI Workshop took place in Bucharest, Romania, in September 16th 2013. It was hosted and organized by Transelectrica, with the support of other CockpitCI partners.

The workshop has taken place into the International Hotel in Bucharest, and has allowed gathering together more than sixty people part of the IT and SCADA security fields and belonging to Critical Infrastructures stakeholders. After the presentation of the main challenge and strategy of the project performed by M. Antonio Graziano, the project coordinator, seven members of the consortium has presented the results and the future tasks of the project in the following topics: cyber-detection, modelling and simulation of cyber threats and services behaviour, prediction of quality of service for interdependent critical infrastructures and smart validation test bed including real and virtual system (hybrid test bed).

Some photos of the Workshop are available on the CockpitCI web-site.

4.4.2 List of overall presentations

Topic	Presenter	Organisation
CockpitCI Project Overview	Antonio Graziano,	SELEX ES S.p.A
The CockpitCI Cyber Analysis and Detection Layer	Tiago Cruz	FTCUC
Integrated Detection Mechanism Dr Leandros Maglaras	Leandros Malgaras	Surrey University
Specific detection tools developed for CockpitCI: Software vulnerability and malware analysis engines	Matthieu Aubigny	itrust consulting
Modelling Loss/False Controllability / Observability of Electrical grids under cyber attacks	Michele Minichino	ENEA
RAO Simulation	Sergei Iassinovski	Multitel
Integrated Risk Predictor in CockpitCI	Stefano Panzieri	Roma Tre
Validation Process Peculiar Properties in the Multinational R&D CIIP Projects. CockpitCI Project Example.	Leonid Lev	IEC

4.4.3 Findings

The workshop gathered more than 60 attendees (mainly from national industry from Romania) who actively participated in the discussions, providing valuable feedback to the CockpitCI Project and good networking and exploitation paths that will be explored in the future. After the workshop presentation, an open discussion with the attendees has been organised and a brief intervention has been made by the responsible of CIs group for Romania to underline the necessity to work together, (stakeholders and governmental authorities) to enhance the level of resilience of the CIs.

4.5 Workshop in Stavanger (Lyse)

The objective of the workshop was to present the results of CockpitCI project to the managers and technical teams of Lyse and to receive feedback on the CockpitCI tools designed within the project. In the first part of the workshop, the CockpitCI concept has been presented. In the second part, selected presentations from CockpitCI partners

provided an overview of the tools implemented in the CokpitCI system. The workshop will finish with a joint discussion panel.

4.5.1 Organisation

The 6th CockpitCI Workshop took place in Stavanger, Norway, in March 20th 2013. It was hosted and organized by Lyse, with the support of other CockpitCI partners.

Its half-day program – included in Annex A – included a set of technical presentations about the CockpitCI Project.

4.5.2 List of overall presentations

Topic	Presenter	Organisation
Improving cyber-security awareness on Industrial Control Systems: the CockpitCI approach	Paulo Simoes	FTCUC
An electrical grid and its SCADA under cyber-attacks: modelling versus a Hybrid Test Bed	Michele Minichino	ENEA
Integrated Risk Prediction: think globally and act locally	Chiara Foglietta	Roma Tre
Quality of service indicators simulation under cyber-attacks using Intelligent RAO Simulator	Sergei Iassinovski	Multitel
The validation methodology for the multinational research projects. CockpitCI project example	Leonid Lev	IEC

4.5.3 Findings

The workshop gathered more than 20 attendees (mainly from Lyse) who actively participated in the discussions, providing valuable feedback to the CockpitCI Project and good networking and exploitation paths that will be explored in the future.

4.6 Workshop in Roma (ENEA & itrust)

The objective of the workshop was both to present the CockpitCI project (overview and tools); the first full-size demonstration of the main CockpitCI system and to have an open discussion on the issues addressed by the CockpitCI project with End Users and System Manufacturers in the Energy, ICT and Control Systems sectors. In the first part of the workshop, the CockpitCI concepts and tools will have been presented. In the second part, selected presentations from industry stakeholders provided an overview of current industry practices. In a third part a demonstration of the CockpitCI system has been performed.

4.6.1 Organisation

The 6th CockpitCI Workshop took place in Roma, in December 16th 2014. It was hosted and organized by ENEA, with the support of other CockpitCI partners.

Its full-day program – included in Annex A – included a set of technical presentations about the CockpitCI Project and a set of presentations from invited international industry speakers. More specifically, the following external speakers were invited to participate:

- ***Cyber Security for Automation Process***, by Antonio Cerilli (Schneider, Italy)

Schneider Electric Corporation (http://www2.schneider-electric.com) is an international company, which provides as industrial leader in ICS, cybersecurity system for Critical Infrastructure. Schneider Electric's integrated cybersecurity solutions for critical infrastructures are best-in-class, allowing users to increase the safety, availability and reliability of Industrial Control Systems:

- Centralize security
- Provide robust change management
- Automate reporting that supports regulatory compliance
- Ensure that only trusted applications run on critical infrastructure environments
- Protect systems from zero day attacks and advanced persistent threats (APTs)

- ***Safe Network Integration***, Shaul Pescovsky (Waterfall Security Solutions, Israel)

Waterfall® Security Solutions Ltd (http://www.waterfall-security.com) is an Israel company specialised in alternative security solution for Critical Infrastructure network. They are the leading provider of strong network security products which protect the safety and the reliability of control system networks. Waterfall Security Solutions' mission is to eliminate the use of firewalls in critical infrastructure control systems. The company develops products which provide stronger-than-firewall protections for industrial control networks. Waterfall's products are deployed in utilities and critical national infrastructures throughout North America, Europe, Asia and the Middle-East.

Some photos of the Workshop are available on the CockpitCI web-site.

4.6.2 List of overall presentations

Topic	Presenter	Organisation
Presentation of ENEA and ENEA research projects	Cristina Corazza & Vincenzo Artale	ENEA
CockpitCI project overview	Antonio Graziano	SELEX
Cyber Analysis and Detection Layer	Tiago Cruz	University of Coimbra
Security assurance of Detection Layer	Moussa Ouedraogo	CRPHT
Integrated Detection Mechanism	Leandros Maglaras	University of Surrey
Detection tools: concrete examples and user guide policy	Matthieu Aubigny	Itrust consulting
Efficiency of electrical grids under cyber attacks on their SCADA	Michele Minichino	ENEA
Grid Quality of Service indicators under cyber attacks	Serguei Iassinoski	Multitel
Integrated Risk Predictor	Chiara Foglietta	Roma Tre
Validation Process in the Multinational R&D CIIP Projects: CockpitCI example	Leonid Lev	IEC
Cyber Security for Automation Process	Antonio Cerilli	Schneider, Italy
Safe Network Integration	Shaul Pescovsky	Waterfall Security Solutions, Israel
CockpitCI Demonstration session	Leonid Lev Stefano Panzieri Tiago Cruz	IEC Roma Tre FTCUC
CockpitCI tool in validation environment	*Leonid Lev*	*IEC, Israel*
Shadow Remote Terminal Unit	*Tiago Cruz*	*FTCUC*
Smart Remote Terminal Unit -	*Giovanni Corbo*	*Roma Tre*
Modelling versus remote hybrid test bed -	*Benedetto Fresilli*	*ENEA*

4.6.3 Findings

The workshop has registered more than 60 attendees (mainly from national industry, graduate students and researchers from Portuguese universities and national organisations) who actively participated in the discussions, providing valuable feedback to the CockpitCI Project and good networking and exploitation paths that will be explored in the future. The demonstration of CockpitCI system has been much appreciated and allowed to collect valuable feedbacks from attendees.

5 Publications, seminars and conferences

5.1 Strategy

Publications, seminars and conference attendances will follow the dissemination strategy described in the figure below.

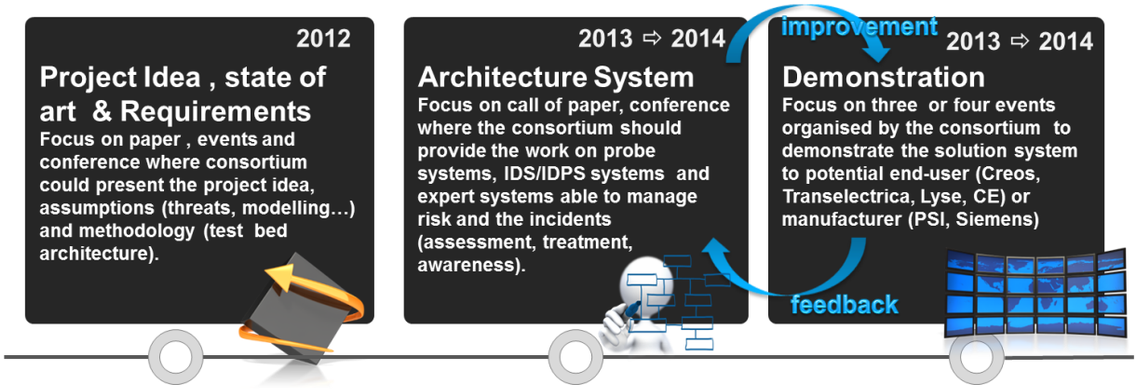


Figure 15: Publications, seminars and conferences dissemination strategy

As shown, the dissemination strategy will include feedback and improvement cycles in order to refine the work-package results and generate end-user and scientific community feedback. We will solicit comments on the architecture and the demonstration in order to make improvements.

5.2 Scientific publications

This Section covers scientific publications in peer-reviewed books, journals, and proceedings of research conferences and workshops.

The following scientific papers are planned to be published in referred books, journals and research conferences and workshops. As CockpitCI is the follow-up project of the MICIE project, the first publications provided during the project will debrief both the results of the MICIE project and their implication on the CockpitCI strategy e.g. how to take into account cyber-security into a Quality of Service risk assessment framework (which has been the main goal of MICIE).

Initially our goal was to submit one paper per quarter. The tentative schedule is was the following:

Q2 2012	Final MICIE results and questions opened by cyber-security issues (ENEA)
Q3 2012	Overview of the project (CRAT)
Q4 2012	Smart algorithm of detection based on behavioural analysis (Bradford)
Q1 2013	Detection framework and detection strategy (FCTUC)
Q2 2013	Malware attack modelling (ENEA)
Q3 –Q4 2013	Attack analysis strategy and risk prediction (itrust, RomaTre)
Q1-Q2 2014	Description of innovative tools designed and implemented during the project (all partners)
Q3-Q1 2015	Description of the project results (all partners)

5.2.1 Funding acknowledgement

All papers written in the context of CockpitCI include an acknowledgement to the funding received from the EU, based on the following sentence: “This work has been carried out in the framework of the CockpitCI project, partially funded by the EU”.

5.2.2 Published papers relative to CockpitCI

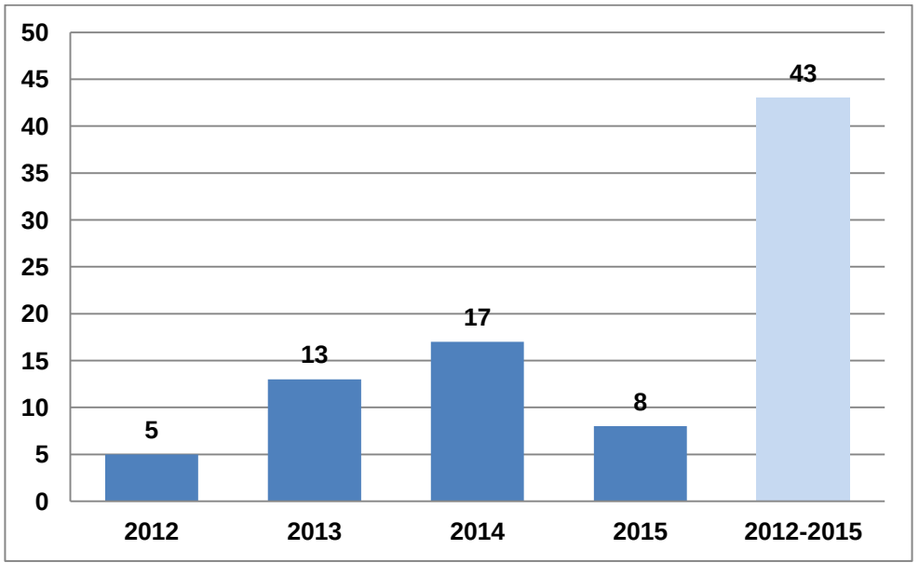


Figure 16: Overview of CockpitCI publications

5.2.2.1 Publications for 2015 (8)

[1] FTCUC: Abstract submitted for book chapter for the upcoming Springer volume "**Recent Advances in Computational Intelligence in Defense and Security**". The proposal, untitled “How to improve cyber-security awareness on Industrial Control Systems: lessons from the CockpitCI project”. (http://www.ieeeottawa.ca/ci/cids-book/)

[2] FTCUC: An paper about CockpitCI is under preparation for the International Journal of Cyber Warfare and Terrorism (IJCWT): title to be defined

[3] Book chapter: F.Caldeira, T. Cruz, P.Simões, and E.Monteiro, “Towards protecting critical infrastructures” in **Cybersecurity Policies and Strategies for Cyberwarfare Prevention**, Editor: Jean-Loup Richet, published by IGI-Global (accepted, awaiting publication).

[4] Book chapter : Paulo Simões, Tiago Cruz, Jorge Proença and Edmundo Monteiro, “**Specialized Honeypots for SCADA Systems**”, in Cyber Security: Analytics, Technology and Automation. Editor: Martti Lehto, Springer Series on Intelligent Systems, Control and Automation: Science and Engineering (2015).

[5] T.Cruz, J.Barrigas, J.Proença, A.Graziano, S.Panzieri, L.Lev, and P.Simões, "*Improving Network Security Monitoring for Industrial Control Systems*", in 14th IFIP/IEEE Int. Symposium on Integrated Management (IM 2015), Ottawa (CANADA), 2015.

[6] L. Rosa, P. Alves, T. Cruz, P. Simões, E. Monteiro, “**A Comparative Study of Correlation Engines for Security Event Management** “, submitted to the ICCWS 2015 conference (abstract accepted).

[7] T.Cruz, J.Proença, P.Simões, M.Aubigny, M.Ouedrago, A.Graziano, and Yasakhetu, L. , "*Improving Cyber-Security Awareness on Industrial Control Systems: The CockpitCI Approach*", Journal of Information Warfare - ISSN 1445 3347 (online) / ISSN 445-3312 (printed), vol. 13, issue 4, 2015.

[8] Carlo Harpes, Matthieu Aubigny, "**CockpitCI: How to monitor cyber-risks on a critical infrastructure**", in Revue Technique Luxembourgeoise, 2015.

5.2.2.2 Publications for 2014 (17)

[9] Francesco Liberati, Andrea Lanna, Donato Macone, Roberto Baldoni, Roberto Cusani, Francesco Delli Priscol, "**CockpitCI: a tool for Critical Infrastructure Protection against Cyberattacks**", International Journal of Critical Infrastructures (http://www.inderscience.com/jhome.php?jcode=ijcis).

[10] André Riker, Tiago Cruz, Bruno Marques, Marilia Curado, Paulo Simões, Edmundo Monteiro, "**Efficient and Secure M2M Communications for Smart Metering**", accepted in the 19th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA'2014), Barcelona, Spain, 16 - 19 September 2014.

[11] Tiago Cruz, Paulo Simoes, Jorge Proença, Matthieu Aubigny, Antonio Graziano, Moussa Ouedraogo, "**Improving cyber-security awareness on Industrial Control Systems: the CockpitCI approach"**, 13th European Conference on Information Warfare and Security ECCWS 2014, At Piraeus, Greece.

[12] Leandros A. Maglaras, Jianmin Jiang, Tiago Cruz, "**An integrated OCSVM mechanism for intrusion detection in SCADA systems**", IET Electronics Letters, Volume 50, issue 25, December 2014, p 1935-1936, DOI: 10.1049/el.2014.2897

[13] Ester Ciancamerla, Benedetto Fresilli, Michele Minichino, Tatiana Patriarca and Serguei Iassinovski, "**An electrical grid and its SCADA under cyber attacks, modelling versus a Hybrid Test Bed**", proceeding of 48th Annual International Carnahan Conference on Security Technology Rome, Italy – October 13-16, 2014, pp. 182 – 187. (ISBN 978-1-4799-3531-4)

[14] S.Iassinovski, M. Minichino E., Ciancamerla, "**Quality of service indicators from simulation of electricity distribution system controlled by SCADA under cyber attacks**". Proceedings of the Congress on Intelligent Systems and Information Technologies "IS&IT'14". Scientific publication in 4 volumes. - Moscou: Physmathlit, 2014, vol. 4, pp 48 - 55 (ISBN 978-5-9221-1572-8).

[15] E. Ciancamerla, B. Fresilli, M. Minichino, S. Palmieri, T. Patriarca "Quality of Service of an Electrical Grid Under Cyber Attacks on its Supervisory Control And Data Acquisition System" ENEA magazine: EAI special issue I 2014 - ENEA technologies for security

[16] E. Ciancamerla, M. Minichino, T. Roman, S. Voronca "**Attack scenarios and expected consequences in SCADA System of a Power Grid**", proceedings of National Symposium on "Informatics, Automation and Telecommunications in Energy, the Tenth Edition - Sinaia, Romania - 22-24 October 2014

[17] Michele Minichino, Maurizio Aiello, Paul MacGregor "**The protection of critical infrastructures: Institutional needs, research and industrial solutions**" invited talk - Horizon 2020:Transforming Global Challenges in Opportunities for Growth - European Parliament, Brussels, 25th September 2014

[18] E. Ciancamerla, M. Minichino "**La Qualita' del Servizio delle Reti Elettriche sotto attacchi informatici ai loro sistemi di Telecontrollo (SCADA)**", invited talk - Cyber Security Energia 2014 - 1° National Conference, Rome - 03 luglio 2014

[19] Leandros A. Maglaras, Jianmin Jiang, "**A novel intrusion detection method based on OCSVM and K-means recursive clustering**", EAI Transactions on Security and Safety, accepted, EAI Transactions on Security and Safety, vol. 2, no 3, e5, pp. 1-10, January 2015, DOI : http://eudl.eu/doi/10.4108/sesa.2.3.e5

[20] Leandros A. Maglaras, Jianmin Jiang, "**A real time OCSVM Intrusion Detection module with low overhead for SCADA systems**", International Journal of Advanced Research in Artificial Intelligence (IJARAI), Vol. 3, No.10, pp. 45-53, October, 2014, DOI: 10.14569/IJARAI.2014.031006

[21] Leandros A. Maglaras, Jianmin Jiang, "**Intrusion Detection in SCADA systems using machine learning techniques**", in proceedings of the IEEE Science & Information conference, London, 27-29 August 2014

[22] Leandros A. Maglaras, Jianmin Jiang, "**OCSVM model combined with K-means recursive clustering for intrusion detection in SCADA systems**", in proceedings of the IEEE Qshine, Rhodes, 18-20 August 2014

[23] Leandros A. Maglaras, Jianmin Jiang, "**Intrusion Detection in SCADA system – CockpitCI project**", in proceedings of the WASET ICAIDM 2014, London, 26-27 May 2014.

[24] Tiago Cruz, Jorge Proença, Paulo Simões, Matthieu Aubigny, Moussa Ouedraogo, Antonio Graziano, Leandros Maglaras, "**A Distributed IDS for Industrial Control Systems**", International Journal of Cyber Secutiry and Terorism (IJCWT), vol. 4, No 2, April 2014, pp 1-22, DOI: 10.14569/IJARAI.2014.031006

[25] M.Ouedrago, C.Kuo, S.Tjoa, D.Preston, E.Dubois, P.Simões, T.Cruz, T. , "Keeping an Eye on Your Security Through Assurance Indicators", in SECRYPT'2014 (11th International Conference on Security and Criptography), Vienna (Austria) 2014

5.2.2.3 Publications for 2013 (13)

[26] Yasakethu, Lasith and Jiang, Jianmin and Graziano, Antonio, "**Intelligent risk detection and analysis tools for critical infrastructure protection**", EUROCON, 2013 IEEE.

[27] Jiang, Jianmin and Yasakethu, Lasith, "**Anomaly Detection via One Class SVM for Protection of SCADA Systems**", Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC), 2013 International Conference on, IEEE, 2013. p. 82-88

[28] C. Foglietta, S. Panzieri, D. Macone, F. Liberati, A. Simeoni, "**Detection and Impact of Cyber Attacks in a Critical Infrastructures Scenario: the CockpitCI Approach**", International Journal System of Systems Engineering, Volume 4, Issue 3, pp. 211-221, 2013, DOI 10.1504/IJSSE.2013.057669.

[29] A.Di Pietro, C.Foglietta, S.Palmieri, S.Panzieri, "**Assessing the Impact of Cyber Attacks on Interdependent Physical Systems**", Critical Infrastructure Protection VII, IFIP Advances in Information and Communication Technology Volume 417, 2013, pp 215-227.

[30] Paulo Simões, Tiago Cruz, Jorge Proença, Edmundo Monteiro, "**Honeypots especializados para Redes de Controlo Industrial",** 7th Iberian-American Congress on Informatics Security (CIBSI 2013), Panama, October 2013

[31] A.Bobbio, L.Egidi, E.Ciancamerta, M.Minichino, R.Terrugia, "**Weighted attack trees for the Cybersecurity analysis of SCADA Systems**", DHSS, 2013 International Defense and Homeland Security Simulation Workshop, Athens, Greece, 25-27 September 2013.

[32] Jiang, Jianmin and Yasakethu, Lasith, **"Intelligent Risk Detection and Analysis Tools for Critical Infrastructure Protection",** accepted for publication in the IEEE Eurocon conference, Croatia, July 2013.

[33] E.Ciancamerta, M.Minichino, S.Palmieri, "**Modelling SCADA and corporate network of medium voltage power grid under cyber attacks**", SECRYPT 2013, Iceland, 29-31 July 2013.

[34] E.Ciancamerta, M.Minichino, S.Palmieri, "**Modeling cyber attacks on a critical infrastructure scenario**", IISA2013, 10-12 July 2013.

[35] P.Simoes, T.Cruz, J.Proença, E.Monteiro, "**On the use of Honeypots for Detecting Cyber Attacks on Industrial Control Networks**", 12th European Conference on Information Warfare and Security (ECIW2013), Jyväskylä, Finland, July 2013.

[36] M.Ouedraogo, M.Khodja, D.Khadraoui, "**Predicting the QoS of Critical Infrastrcurture trough Analysis of the Cyber Security Vulnerabilities**", ARES-RISI 2013 Workshop.

[37] Jiang, Jianmin and Yasakethu, Lasith, "**Computerized risk detection towards Critical Infrastructure Protection: An Introduction of CockpitCI Project**", Proceedings GV, ISBN: 978-80-554-0649-7, ISSN: 1339-2778, vol. 1, issue 1, pp. 602--606, 2013

[38] Jonathan Blangenois, Guy Guemkam, Christophe Feltus, Djamel Khadraoui, **"Organizational Security Architecture for Critical Infrastructure"** (ARES-FARES 2013 workshop)

5.2.2.4 Publications for 2012 (5)

[39] Lasith Yasakethu, Jianmin Jiang, "**Real-Time Intrusion Detection for Critical Infrastructure Protection: CockpitCI Approach**", eForensics magazine-Network, Vol-1, No-4, pp18-25, December 2012.

[40] M.Castrucci, E.Ciancamerta, F.Delli Priscoli, S.Iassinovski, F.Liberati, D.Macone, M.Minichino, S.Panzieri, A.Simeoni, "**Detection of and reaction to cyber attacks in a Critical Infrastructures scenario: the CockpitCI approach**", International Defense and Homeland Security Simulation Workshop, Vienna, Austria, 19-21 September 2012.

[41] E.Ciancamerta, M.Minichino, S.Palmieri, "**Cyber attacks spreading and impact on QoS of SCADA**", CRITIS 2012, Lillehammer, Norway, 17-18 September 2012.

[42] E.Ciancamerta, M.Minichino, S.Palmieri, "**On prediction of QoS of SCADA accounting cyber attacks**", Probabilistic Safety Assessment and Management Conference (PSAM11) and the Annual European Safety and Reliability Conference (ESREL 2012), Helsinki, Finland, 25-29 June 2012.

[43] A.Bobbio, A.Bonaventura, E.Ciancamerta, D.Lefevre, M.Minichino, R.Terrugia, "**Temporal network reliability in perturbed scenarios: Application to a SCADA system**", in procceding IEEE Annual Reliability and Maintainability Symposium, RENO, 2012.

5.3 Participation in Seminars, Meetings and other events

5.3.1 FTCUC

The following paragraphs describe the meetings with the Industry conducted by University of Coimbra to present the CockpitCI project:

- **EDP/Univ. of Coimbra Brainstorming Workshop, EDP-Coimbra (April 10th, 2013)**

In the context of a private brainstorming workshop jointly organised by University of Coimbra and EDP, the CockpitCI Project was presented by the University of Coimbra.

As already mentioned, EDP is the largest utility in Portugal. The aim of this workshop, attended by a significant part of the EDP staff involved in innovation and research projects, was to discuss and identify opportunities for future applied research and technology transfer projects involving the University of Coimbra and EDP. CockpitCI was one of the projects presented in this workshop, and the applicability of its concepts and outcomes was analysed.

- **EDP Headquarters, Lisbon (April 23rd, 2013)**

Following the presentation of the CockpitCI project, in the abovementioned April workshop, EDP invited the University of Coimbra for a meeting at its headquarters, in Lisbon, to specifically discuss how the results of CockpitCI could be used to improve the security of EDP distribution networks and to process the SCADA events generated by its HV/MV distribution grid (including security issues but also monitoring and operations support in general, based on the capabilities of the event processing and correlation mechanisms being developed for CockpitCI).

- **Lecturer 2013 to CrIM 2013**

UC provided an invited lecturer (Tiago Cruz) for the Seventh International Crisis Management Workshop (CrIM'13) and Oulu Winter School, held at the University of Oulu (Finland) between November 25th and November 26th 2013. The title of the presentation was "CockpitCI Cyber Analysis and Detection Layer".

(https://www.ee.oulu.fi/research/ouspg/CrIM13)

5.3.2 ENEA

On September 25th 2014, Michele Minichino has been invited by the Italian Embassy at Bruxelles to contribute to the event "*Open, Safe and Secure Cyber Space. New Security frontiers beyond technology*" (http://www.techitaly.eu)

During the round table titled "*Institutional needs research and industrial solutions*", in the framework of MICIE and CockpitCI projects, he presented and discussed the following topics:

- A Critical Infrastructure (electrical grid) & SCADA under cyber attacks
- How to Model cyber-attacks and their propagation on SCADA
- How to measure attack consequences on SCADA and the physical Critical Infrastructure itself
- Any major challenge and limits in modelling approach
- How to emulate cyber-attacks and to measure their consequences by means of a hybrid test bed
- Could Decision Support Systems assist SCADA operator in preventing cyber-attacks and in mitigating their consequences

During the Roma Workshop organised by ENEA, interviews for specific journals and Internet TV has been made to increase the dissemination of the CockpitCI concepts and results (Full text are in Annexe A):

1. Internet TV interview of Antonio Graziano: http://webtv.enea.it/Members/webtvadmin/videos/CockpitCIfinal.mpg
2. Ufficio-stampa_ENEA_facebook
3. Energia_ progetto ENEA per rafforzare sicurezza reti
4. 17/12/2014 COMUNICATI STAMPA "*Energia: progetto ENEA per rafforzare sicurezza reti in collaborazione con Selex (Finmeccanica) e partner europei e israeliani*".

5.3.3 itrust consulting

During the Luxembourg Workshop organised by ENEA, interviews for specific journals has been made to increase the dissemination of the CockpitCI concepts and results:

1. Revue technique Luxembourgeoise / Internet press paper March 2014
2. IT One 25 March 2014 : "Scada Cybersecurity Workshop" http://www.itone.lu/article/scada-cybersecurity-workshop
3. 18.03.2014 "Cybersecurity de système de contrôle SCADA": http://www.creos-net.lu/actualites/actualites/article/cybersecurity-de-systeme-de-controle-scada.html
4. Paperjam March 2014

5.4 Attendance to international conferences

Conferences are the events where we expect to reveal the innovative concepts or to present the resulting product of the CockpitCI project to potential stakeholders. This section also considers similar events that occur during the project, such as seminars, workshops, etc.

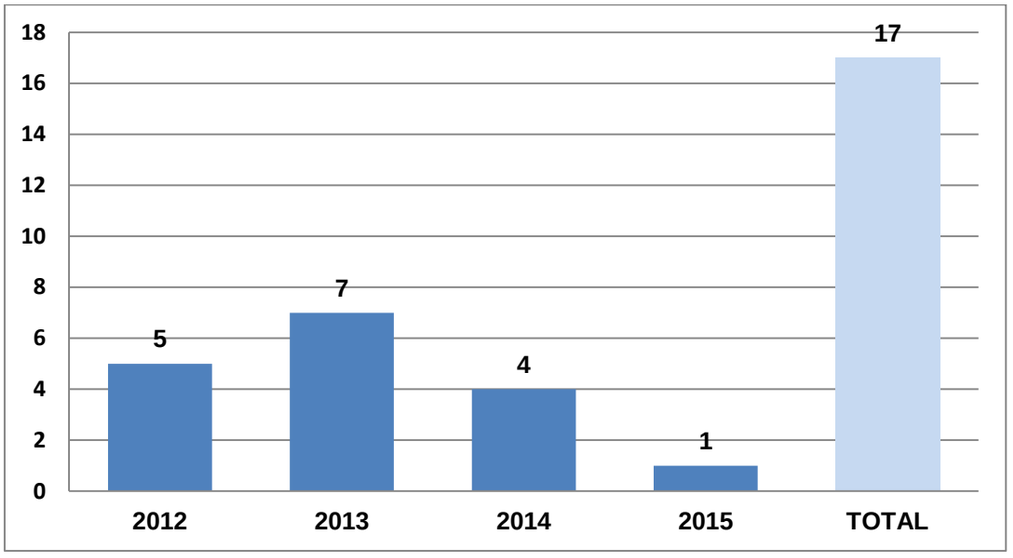


Figure 17: Overview of CockpitCI attendance to international events

Here we present a list of events as well as some details for each one. The decision to participate in a conference was dependent on factors such as the match between the conference topics and the subject of the innovation or the availability of relevant results at the time of the conference.

Date	Event	Consortium Attendance
25-29 June 2012	Probabilistic Safety Assessment and Management Conference (PSAM11) and the Annual European Safety and Reliability Conference (ESREL 2012) - Helsinki, Finland	ENEA
17-18 Sep 2012	CRITIS Conference on Critical Information Infrastructures Security, Lillehammer (Norway)	ENEA
19-21 Sep 2012	International Defense and Homeland Security Simulation Workshop (DHSS2012) Wien - Austria, September 2012	ROMA3
23-25 Oct 2012	hack.lu 2012, Luxembourg	itrust
23–25 Oct 2012	Informatics, Automation and Telecommunications in Energy – Symposium Sinaia Romania	Transelectrica
18-20 March 2013	Seventh Annual IFIP WG 11.10 International Conference on Critical Infrastructure Protection (Washington)	ROMA3
April 2013	The Global Virtual Conference 2013 (GV-CONF 2013), Goce Delchev University Macedonia & THOMSON Ltd. Slovakia	SURREY
24-27th June 2013	43rd Annual IEEE/IFIP International Conference on Dependable Systems and Networks, Budapest	ENEA

1-4th July 2013	IEEE Eurocon conference, Croatia	SURREY
11-12th July 2013	12th European Conference on Information Warfare and Security (ECIW 2013), Jyväskylä, Finland	FTCUC
11-12 September 2013	International Conference on Availability, Reliability and Security, Regensburg, Germany	CRPHT
23-25 October 2013	The National Power Conference and Exhibition (CNEE 2013), Sinaia, Romania	Transelectrica
29-31th October 2013	7th Iberian-American Congress on Informatics Security (CIBSI 2013), Panama	FTCUC
12-14 March 2014	Cigre Belgium 2014: Innovation For Secure And Efficient Transmission Grids	Roma3, FTCUC, itrust
22-26 June 2014	FOREN 2014: 12th World Energy Council Central and Eastern Europe Regional Energy Forum (Bucharest, Romania), IEC	Transelectrica
22-25 July 2014	KIE Conference “Knowledge-informed science, technology and business innovation”, Riga, Latvia	SURREY
27-29 August 2014	IEEE Science & Information conference, London, Great Britain	SURREY
24-26 March 2015	CyberTech conference – Tel Aviv	IEC

Table 2: List of Conferences

6 Exploitation plan

6.1 Starting point: stakeholder analysis

The exploitation plan considered the definition and expectations of companies that will be able to pay for the CockpitCI product (final development and deployment as a software/hardware package).

The objective is to collect their potential interests and expectations, check a convenient business model, etc.

Stakeholders include:

- Professional partners such as IEC, Lyse and Transelectrica;
- Expected stakeholders for the tools such as manufacturers like PSI, Siemens, etc.;
- Electrical providers such as CREOS (part of the advisory board of the project), EDF, etc.

As mentioned above, most of the stakeholder analysis was performed trough personal meeting at the occasion of workshops or international conferences. This meeting allowed underlining that the CockpiCI system could improve the security of CI managements even if the cyber awareness still remains weak to face to the real and present threat.

6.2 Expected exploitation plan

The following paragraphs gives an overview of the expected exploitation plan of the CockpiCI as it has been foreseen in the Do Work of the project.

"*The results of the project can be exploited along the following paths:*

- *Products and solutions: The results of CockpitCI will lead to the development of new products, especially in the fields of smart detection agent and analysis tools, and solutions which address the security of CI.*
- *Services: The Demo System will have the potential to be exploited. That could be the base for IEC and other end-users to provide new features to their control systems and assure more reliable services to their users.*
- *Consultancy: Through CockpitCI partners will acquire skills in the area of Cyber attacks analysis, Interdependency Analysis, Risk Prediction, Modelling and Cross CI's domain data security. It is only natural for all partners to exploit these skills in the acquisition and execution of future projects.*

Other avenues of exploitation include the ongoing development of technologies within all of the consortium partners; these technologies may have widespread applications beyond public security".

This description the background of the exploitation plan followed by all partners during the project and still remains a useful guideline for the next step of the research beyond the CockpitCI project. This background has been also taken into account when the consortium defined the strategy of exploitation. The following paragraph gives a chronological overview of the exploitation plan: first at mid-term review (as it has been presented to the project officer), secondly at the end of the project both for specific partners and for the consortium taken as a whole.

Note: The CockpitCI consortium includes research laboratories, research company or university which are not interested or allowed to exploit results in a commercial strategy. Therefore, the exploitation plan, at the end of project, does not deal the exploitation plan of all partners.

6.3 Exploitation plan at mid-term

6.3.1 Strategy followed

According to the presentation provided during the mid-term review, the consortium have been set up a strategy to guide the exploitation plan of the project.

The strategy for the exploitation plan was to focus dedicated action according to the following two phases:

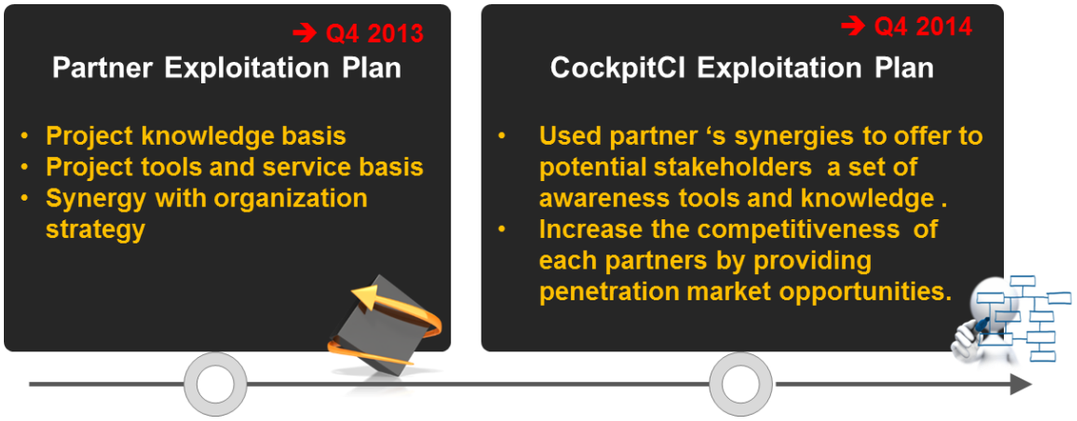


Figure 18: Strategy of exploitation plan

6.3.2 Partners' exploitation guideline according to the mid-term findings

6.3.2.1 IEC

The hybrid test bed will be used by IEC in a more global view to increase security awareness on ICS monitoring and CIP and to propose an easy sand box for testing campaigns of systems deployed on relative systems and networks.

6.3.2.2 FCTUC

At mid-term, the University of Coïmbra has built its own exploitation plan on 5 pillars as follow:

- Exploitation of the new technology of Shadow RTU, which should lead to patent and could be spread in other ICS context.
- Publication paper on CockpitCI results and follow-up ideas as Smart RTU.
- Strength links with partners and stakeholders as EDP (Portugal electrical corporation)
- Use the acquired knowledge to propose new research topics in cyber-security and participate to security project.
- Reinforce position in several research initiatives as COST Action [Intellicis COST Action IC0806], and thematic networks [SysSec Network of Excellence and CRIPTORED]

6.3.2.3 Selex ES

At mid-term of the project, Selex ES expected to fine-tune the identified exploitation lines i.e.

- SCADA business line (direct project exploitation): market dedicated to low-cost smart devices and of QoS simulation under cyber-attacks tools

- Cross-Business line (indirect project exploitation): market dedicated to cyber modelling for different type of network systems and development opportunities of adaptive systems for central and peripheral reaction system and process.

Moreover, Selex ES have planned to perform technical reviews and business reviews of the ideas and set up a business packages for each one if the idea is sustainable

6.3.2.4 itrust consulting

At mid-term of the project, itrust consulting planned exploit the results of the project into four directions:

- Provide security services designed during the project to stakeholders (CREOS, Governmental organization…) inside a CERT: CERT-malware-lu.
- Use the acquired knowledge to propose new research topics in cyber-security at National [SGL-Cockpit on security of smart metering systems] and European level.
- Increase knowledge on real-time risk assessment methodology and tools to apply to general risk assessment in ICT domain
- Provide expert analysis and inputs for standardization organization (ISO/JTC1)

6.3.2.5 CRPHT

The exploitation plan of the CRPHT at mid-term of the project, lay on five blocks:

- Develop a methodology and tool to help predict QoS parameters.
- Enhance existing tools on Security and risks monitoring.
- Exploit results of the project especially on the risk prediction in ICS to reach out to stakeholders in the energy sector in Luxembourg.
- Open a new line of research on CIP within the research centre.
- Provide a professional master training course in the domain of security of interdependent systems.

6.3.3 Conclusion at mid-term

The continued relevance of the objectives and breakthrough potential with respect to the scientific and industrial state of the art

1. The continued relevance of the objectives
   - The issue of cyber security in the SCADA field is more than ever actual (Stuxnet, Duqu etc.).
   - The importance of Critical Infrastructure in everyday life is true more than ever.
   - Pursuing awareness is important for all (cyber operator, scada operator, managers,..) to make better and more comprehensive decisions.
   - Reaction, addressed as a means to make the system more resilient and adaptive, is potentially very important and at the forefront of research.
   - The results, both in term of methodology and designed systems or process, reached during the project will be easily transposable to other domain such as gas transportation or even telecommunication network.
   - The designed and test of new methodologies, systems or processes in this project will allow European organizations (especially governmental organizations) to have their own cyber defense strategy non depending on extra-European products. This point is the basic condition to avoid cyber-attacks which can come from any countries in the world.
2. Breakthrough potential with respect to the scientific and industrial state of the art

The overall CockpitCI concept still remains ambitious, complex and highly innovative. Single parts of the project which provide a breakthrough are also:

- Shadow RTU (patent is formally envisaged);

- Promising approaches for SMART RTU (if further analysis is positive demonstrator may be implemented);
- HTB could be used to increase the resilience of CIs and could be used in other projects.
- A new strategy of awareness and defense: Systems of detection and analysis, either designed as innovative systems (shadow RTU) or developed and implemented by trusted third party (e.g.: total antivirus service, software checker) can be a keystone for improving the security of CIP and CIIP often depending on the system manufacturers. Linked with algorithms and systems of simulation and prediction developed during the project, these trusted systems will allow organization to assess the real risks of their CIs.
- cyber simulation, no commercial solution capable.

3. Forthcoming exploitation plan issues.
   - To define or fine-tune information exchange standards about security events, security incidents and risk level, to increase the global awareness through the entire Europe by sharing in real-time sensitive information in the respect of privacy and business strategy.
   - To define and formalize FSIR scenario in presence of cyber-attacks.

6.4 Final exploitation plan

At the end of the project, most of expected partners' exploitation plan based on the project results have been reached or still remain reachable in the future. Some have had to be redefined to be in line with end-users expectations or to be in line with market of security systems (cf. partners' exploitation plan)

However, as shows the feedback provided by potential end-users during the demonstration of the CockpitCI tools and workshops organised by partners, the exploitation of the CokcpitCI project, especially from a commercial point of view, requires performing additional research and real-size tests to be able to propose a usable solution, easy to deploy and manage for futures end-users: that is the main objective of a new project follow-up.

6.4.1 Partners' exploitation plan

6.4.1.1 For the University of Coïmbra

The benefits from UC participation in the CockpitCI Project are manifold.

First, the direct cooperation with top-level academic and industry partners provided a stimulating and fertile environment for the UC team which – by means of collaborative research – was able to extensively complement and expand its core set of security-related competencies. Achieved results are quite valuable per se – resulting in a number of scientific papers authored or co-authored by UC researchers – and follow-up research activities with some members of the CockpitCI consortium are also expected in the near future. Joint research is already under way with CPRHT, on Trust and Security Models for CIP, and with University of Surrey, in the field of anomaly detection.

Second, the CockpitCI Project became a key component of UC portfolio on security-related research, complementing its previous experience (focused on communication networks and telecommunications) with novel application fields, such as power utilities, industrial control networks and critical infrastructures in general. This allowed UC to reinforce its position in a number of initiatives – such as COST Actions like Intellicis (COST Action IC0806) and ACROSS (COST Action IC1304) – and to seed new joint research and innovation partnerships based on the scientific outcomes of CockpitCI – two new H2020 project proposals were already prepared.

Furthermore, this allowed UC to increase its cooperation with national and international industrial players in the energy management field, such as EDP (the largest Portuguese electric utility), PT Inovação (the research unit of the largest Portuguese telecommunications company), Galp Energia (oil and gas extracting, refining, distribution and retail) and ISA (an award-winning SME specialized in Telemetry and Machine-to-Machine communications),

resulting in a number of new collaborative projects. FCTUC plans to further exploit potential opportunities for applied research and for the direct provision of innovation and consultancy services to the industry.

Last but not least, the CockpitCI Project contributed to the UC post-graduate teaching activities, strengthening its expertise in the areas of monitoring and security management in industrial networks, with a number of benefiting M.Sc. and Ph.D. students. Luís Rosa and Jorge Proença, members of the UC team, are expected to conclude their PhD in Q2/2015 with theses that are partially based on CockpitCI-related research. Furthermore, CockpitCI provided the research context for 4 MSc theses.

6.4.1.2 For Selex ES

During the first half of the project Selex-ES has been evaluating the maturity of the various parts of the system in order to determine which could be more rapidly and effectively be included into a new offer. Selex has also encouraged UC to submit the patent request for an innovative field device, it has contributed to survey the related state-of-the-art and has discussed with UC the possibility to submit a joint patent; it was finally decided that UC would submit the patent request on their own[1]..

At the end of the second half of the project, Selex has produced a revision of its exploitation plan in order to take into account the project results at the current moment and the maturity achieved by the various parts of the project.

Selex has identified the following two main conceptual exploitation lines:

- **SCADA business line**: Concepts / techniques / models and devices which can contribute to increase in the short / mid / long term the current Selex offer in the SCADA domain;
- **Cross-Business line**: technologies which may be mutuated and transposed in another context to benefit Selex business domains ranging from military to civil;

Regarding the SCADA business line, several technologies have been identified as of potential interest and most promising:

- Innovative low-cost smart devices which may be deployed in the field;
- QoS modelling and simulation in presence of cyber attacks.

Regarding the cross-business line, several technologies have currently been identified as most promising:

- Cyber modeling which has a wide applicability to any system composed of hosts, networks, etc.;
- Cyber detection techniques allowing its future products to better detect, localize both well-known and unprecedented attacks from cyber domains
- Coordination of local and centralized reaction in order to develop more adaptive systems which may exhibit a higher level of robustness and graceful degradation;
- Risk monitoring and risk assessment algorithms whose implementation allows to mitigate the effects of cyber attacks
- Low-cost secure exchange mechanisms for further enhancements, modifications and tailoring of company's security related products thus improving the company's competitiveness in the security domain.

For each of these technologies Selex will perform, according to its internal procedures and business practices, the following activities:

- Technical reviews in order to verify the technical feasibility, maturity and costs of the technology, the possibility to experiment the technology in its own SCADA labs;
- Business reviews in order to verify the economic feasibility of the potential business, i.e. verifying which business would benefit from the investment, the existence of a potential market for the technology, value of the investment, the capability to provide a return on the investment, etc…

[1] The patent was finally not submitted for strategically reasons belong to the University Advisory Board

On a half-yearly basis it will be decided for each technology if one of the following applies:

- Stop, i.e. the conditions are so that it is not worth considering the technology as a potential investment;
- Continue monitoring;
- Promote the technology from the tentative level to the confirmed level.

In the next months for those technologies which have not been dismissed along the way, Selex will produce a business package, according to its own internal procedures, which identifies:

- Scope of the investment;
- Exploitation steps and work plan;
- Liaison with other partners and responsibilities;
- Investment value
- Duration of the investment;
- Commercial returns.

The Business Package will then undergo to the evaluation of top management board.

6.4.1.3 For itrust consulting

Based on the knowledge acquired during the project, itrust consulting succeeded to start a national project on the assessment of smart-meter security for the Luxembourgish electrical provider CREOS. This new project allowed itrust to establish strong relationship with the research laboratory of the University of Luxembourg in charge of ICT and ICS security (SNT).

Moreover, the CockpitCI project allowed itrust to develop two detection tools (one meta-antivirus and one vulnerability software checker) which itrust plans to package into business services or product, not only for electrical provider but for ICT companies or final end-users. In that aim itrust will study the following opportunities in the future:

- Develop the vulnerability detection tool for patch management in ICT environment (for small and medium companies of cloud services).
- Increase the deployment of the meta-antivirus AVCaesar as a security service among CI stakeholder and in dedicated SOC. The service has been setup as a free service for test purposes on https://avcaesar.malware.lu/ itrust consulting hopes to acquirer regular customers willing to scan their confidential data on this service.

According to exploitation plan set up at mid-term of the project, itrust would enforce the cooperation with consortium partners to improve its own Risk Assessment tool (base on ISO 27001) into a real-time and risk prediction tool to allow top management to take tactical decisions and increase the confidence of end-users on their Information System.

Another field included in the future exploitation plan of itrust is the application of the CockpitCI system to the new emergence of smart grid in Europe and first in Luxembourg: the full deployment of smart-meter foreseen on 2015 is the first step of a smart grid deployment in line with European expectation on smart Energy deployment.

6.4.1.4 For IEC

IEC will use the HEDVa results for development of the validation environment for the Israel Smart Grid (ISG) consortium for validation of different smart grid components. In addition the HEDVa results will be used while development of the SCADA part of Israeli government environment for validation of the research projects of universities and SME in Israel.

The CockpitCI project results were presented during the CyberTech conference hold in Tel Aviv on 24-26 March 2015

6.4.1.5 For Transelectrica

The hybrid test bed model will be developed by Transelectrica in National Dispatcher Center to increase security awareness on monitoring EMS/SCADA System and to propose an easy sand box for testing campaigns of systems deployed on relative systems and networks.

6.4.1.6 For Lyse

Although the results of the CockpitCI project have been well received especially trough the demonstration of the tools performed during the Workshop in Stavanger, the management of Lyse has decided to postpone the decision to exploit the CockpitCI system or the methodology for their own electrical infrastructure. Additional studies on the opportunities of exploit these results will be performed in the future.

6.4.1.7 For Multitel

Multitel will explore the simulation models developed during CockpitCI on consulting services to European companies. Nowadays Multitel offers services on computer based simulation and optimization for Belgian industries and European companies in the Railway domain. The CI models developed during CockpitCI can also be customized to railway specific scenarios were networks from different countries need to communicate and react to potential risks like accidents and cyber attacks or simple scheduled work interruptions on their train tracks. The simulation model developed in the context of CockpitCI WP2000, linked to GPS coordinates and a multi-layer network, seems very promising for geographically dispersed but interconnected networks like railway and electricity. Multitel can also offer consulting services on the quality of service prediction under different scenarios of functioning, helping industrial companies to improve their SCADA procedures, SCADA and communication network hardware structure with the goal to increase their resilience with respect to various adverse events like cyber attacks and others.

On the basis of valuable experience and competences acquired with their participation in the CockpitCI project, Multitel is now participating in preparation of new project proposals in the field of critical infrastructure assessment (not limited to electricity). On of such a proposals is IDSS-Water project with the title "Innovative Decision Support System for Water Industry" to be submitted in the frames of work program H2020-WATER-2015-two-stage/WATER-1b-2015.

6.4.1.8 For Roma Tre

Roma TRE will exploit the results of the project in several ways considering the different impacts of all the developed technologies. From the scientific point of view also, the improved approaches to interdependency modelling will be used in developing and analysing scenarios that are more complex and the CISIApro approach will be used to automatically generate the required models. Such improved capabilities will be used in new EU project as well as in developing risk models for Italian infrastructures. The CISIApro platform, made available on the web (www.cisiapro.com) has changed the designing time in a meaningful way and will become, hopefully, a reference platform for interdependence modelling. Form the point of view of cyber-physical systems design and analysis, new methodologies for data-fusion have been developed and will be used to estimate new impacts on electrical and gas infrastructures. In general, situation awareness in the management of smart grids including GAS will be proposed in the URANIUM CIPS (http://uranium.theorematica.it/) project that is coordinate by ROMA TRE. Do not forget that the Integrated Risk Predictor developed by ROMA TRE is able to redefine the QoS of the delivered services and then, a strong economic impact is expected in using such systems in the future.

The SMART Extension, that has been developed during the CockpitCI project, will be proposed as a solution for improving security of traditional RTUs and a spin-off of ROMA TRE will be probably created to exploit such results.

6.4.1.9 For ENEA

ENEA is mainly called upon:

- to promote and carry out basic and applied research and innovation technology activities, also through prototypes and product industrialization;
- to disseminate and transfer technologies, encouraging their use in productive and social sectors;
- to provide high-tech services, studies, tests and evaluations to both public and private bodies and enterprises;
- to collaborates with national and local administration to define research programs and manage research activities.

To these aims and in the sectors falling within its areas of competence, ENEA:

- carries out complex research, development and demonstration projects, mainly technology and engineering — based, sets up and operates major scientific apparatus;
- assesses the level of advanced technologies development, as well as their economic and social impacts, also on demand by public administrations;
- promotes collaboration with foreign bodies and institutions, also for defining technical regulations and participation to major research programs and international organizations, providing its (specific)expertise;

ENEA is in charge to carry out R&D activities on the new frontiers of modelling methods and tools for reliability/dependability evaluation, with current emphasis on modelling and analysis of large complex interconnected systems. The focus is on the investigation of risk based methodologies, qualitative and quantitative indicators, multi formalism and multi solution methods and tools for Quality of Service measures (in terms of performances, reliability and dependability) of large interconnected technological networks, including power grids and telco networks at regional/national level. ENEA takes part in many European Commission initiatives focused on ICT applications on energy and telecommunication sectors within the framework of Critical Information Infrastructure Protection (CIIP). In such a respect, in CockpitCI project, the following additional exploitation aspects have been gained:

- raised awareness and gained knowledge on Telco network and Power grid an SCADA interdependencies and on the possible electrical outages caused by cyber attacks
    - to be used for improving network analysis and/or developing new tools to help in an early detection of interdependency problems and cyber attacks on SCADA to limit future black-outs
    - to be used for training opportunities for researchers, utilities' technicians as well a for industry for further research
- development of advanced simulation tools that allow quantification of impact of interdependencies and cyber attacks:
    - scenarios identified enable to demonstrate interdependencies and effectiveness of remedial actions on cyber attacks
    - high-skilled consultancy to detect cyber attacks versus interdependencies
    - training opportunities for researchers, utilities' technicians as well a for industry
    - perspectives of commercialising ENEA software as add-on in network analysis software

Results gained within CockpitCI project are very valuable for promoting and carrying out applied research and innovation technology activities. Particularly, ENEA testbed linked with IEC testbed and the demonstration of the

main models developed inside WP2000 modelling activities are hosted within ENEA labs. The first activities to be performed are to submit the demonstrators to a deeper testing process in order to better focus on their current characteristics and possibly enhance the robustness of their behaviour. The resulted ENEA environment will be a leverage for the Italian stakeholders in electrical field (i.e. TERNA, ACEA,ENEL) and telecommunication field (i.e. Telecom Italia, Telecom Italia Mobile) for approaching the complex aspect of interdependency among such sectors, in terms of better comprehension, representation and investigation on how they can impact on service delivery.

Moreover, the following exploitation aspects are worthwhile to be highlighted:

- the CockpitCI modelling approach has been extended to represent and predict efficiency and resilience of interdependent smart grid, gas and water networks of the city of Catania (SINERGREEN project funded by italian government: 15 M€)
- the modelling approach intends to be extended to assess and propose solutions for resilience in the modernization process of CI and their SCADA against current challenges (smart metering, efficiency improvement, new paradigms and architectures for SCADA), within a proposal for Horizon 2020
- a Simulation Centre, to predict efficiency and QoS of physical CI their SCADA against adverse events, including cyber attacks, geographically distributed among three ENEA laboratories: Rome-Casaccia, Palermo and Bari, has been built and it is running.
- a hybrid modelling enviroment (hw/emulators/simulators) for CIP under cyber attacks has been built and it is running at ENEA Casaccia, remotely connected to IEC hybrid test bed and Coimbra University.
- ENEA and university researchers, located in sud Italy (Palermo & Bari) improved their awareness in SoS, CIP, SCADA and in the limits and in the challenges of the related modelling techniques
- a small group of ENEA young researchers have been funded and teached making leverage on the project funding and its research arguments

6.4.1.10 For CRAT

Participation in the CockpitCI project has brought and will bring to CRAT many benefits:

- Strengthening of connections with SMEs, industries and research/academic institutions active in the field of security and critical infrastructure protection. Such connections are being exploited and will be exploited more and more to set-up joint initiatives in the field (e.g. submission of proposals to relevant H2020 calls).
- Deepening of CRAT competencies and knowledge in the security and critical infrastructure protection sectors, exploited to upgrade courses held by CRAT personnel at the “Sapienza” University of Rome, and resulting in the possibility for BS, MS and PhD students to get in contact with the latest research topics in the field (with deriving positive outcomes in terms of occupation of young engineers).
- Inspiration and contribution to the set-up of research laboratories and centres such as the “Cyber Intelligence and Information Security” (CIS) research centre at the University of Rome "La Sapienza", the "National Laboratory of Cyber Security" (an inter-university laboratory including all the main Italian universities involved in the cyber security topic) and the SERIT (“Security Research in Italy”, in which CRAT is involved in the Guide Sector 2 – Security of Energetic Infrastructures, and in the Technological Area 2 – Communications).

6.4.1.11 For University of Surrey

University of Surrey during the CockpitCi project managed to produce innovative intrusion detection models. These models where fully implemented, producing self-executable distributed agents that can be employed in any system after proper training and parameter tuning. Based on these products, University of Surrey has already established

collaboration with University of Coimbra, IEC and De Montfort University with main target the creation of adaptive intrusion detection agents that can be self-tuned and easily integrated in any network based Intrusion Detection System. University of Surrey is also trying to establish cooperation with major companies in the field of Cyber Security (e.g. Airbus Group) in order to test the model in industrial control systems that drive Critical National Infrastructures under different attack scenarios.

6.4.1.12 For CRPHT

A further update of the exploitation plan as the project ends can be summarised as a fruitful venture that offers the opportunity to the institute to reinforce existing expertise in the field of Critical Infrastructure and also open some avenue for further collaboration with consortium members and new research opportunities.

Indeed CockpitCI has helped to further the understanding of energy transmission and distribution infrastructure and the security challenges it faces. Critical Infrastructure Protection (CIP) has been incorporated within the centre as a salient research topic and the team is being developed for a more thorough analysis of the peculiarity of CIP. The security assurance platform of the detection layer that has resulted from the project can be applied in numerous application domains. While in CockpitCI the focus was primarily on energy infrastructure, Tudor intends to explore the application of the philosophy of security supervisory other types of infrastructure such as transport and Telecommunication.

Tudor will seek further maturation of the platform, especially with respect to its practicality in real cases involving complex heterogeneous infrastructure and some opportunity to do so may come under the series of call on Innovation Action of the H2020 program.

Besides addressing the challenges of the CocpitCi, a number of interesting collaborative work and project have been initiated with some consortium partners and such collaboration will include joint research work and PhD supervision. Tudor has also taken steps to further its links with the University of Luxembourg in view of jointly engaging in the CIP that could directly benefit national operators, Energy and Telecommunication, in particular.

6.4.2 Exploitation plan for the consortium

The most important decision of the consortium regarding the exploitation plan of the CockpitCI project for the future is the unanimous decision to set-up a follow-up project to achieve the development of tools in order to provide for the customers a “commercial” product. Indeed, this request was one of the requests collected during the workshops and demonstration of the CockpitCI tools. Even if the demonstration showed that consortium succeeded developing an interesting set of tools, the following and relevant issues still remains open for a new project:

1. Most of the tools need to be test on a real-size infrastructure to evaluate the performance of the tools and to be fine-tuned.
2. The modelling tools developed during the CockpitCI project is not closely integrated into the entire chain of risk assessment provided by the detection framework and the risk prediction tool. The new project should integrate this different type of approaches to provide more and reliable information for the operators (e.g. integration of the virus spreading modelling to provide inputs for the prediction tools).
3. The link between the detection framework and the risk prediction tools need to be deeply study to provide automatic matching methodology and rules between the detection and analysis of cyber-attacks information and information on QoS of systems under attack.
4. CockpitCI tools, to be efficient, needs to be based on the precise description of the real topology of the environments (operational, SCADA, Telecommunication networks) and on the precise rule of incident management (FSIR scenarios). These elements has been set up step by step during the project but, in the perspective of the commercial deployment of the system, this description should be based on methodology and specific tools to provide a quick and reliable solution.

In order to achieve these identified improvement, the consortium plan to propose a new project in the European H2020 framework. The consortium has identified the following European project calls suitable for a follow-up project:

Digital Security: Cybersecurity, Privacy and Trust

H2020-DS-2015-1 — Sub call of: H2020-DS-2014-2015

Planned Opening Date	25-03-2015		
Publication date	11-12-2013	**Deadline Date**	27-08-2015 17:00:00 (Brussels local time)
Total Call Budget	€50,210,000	**Main Pillar**	Societal Challenges
Status	Forthcoming	**OJ reference**	OJ C 361 of 11 December 2013

Topic: **The role of ICT in Critical Infrastructure Protection** **DS-03-2015**

Specific challenge:

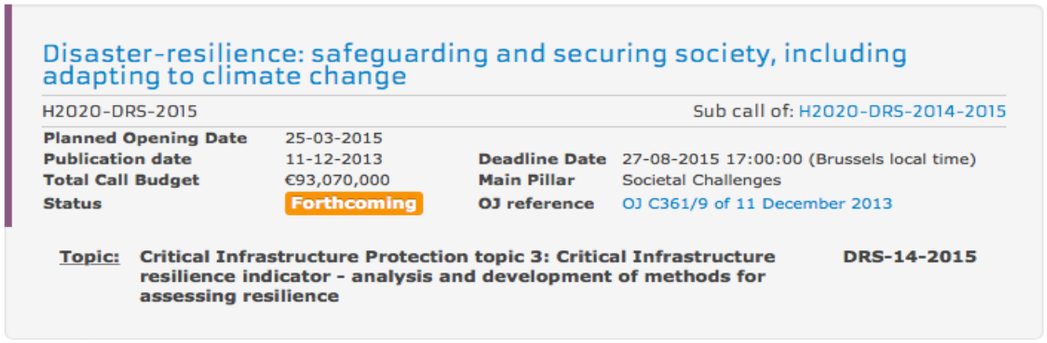
Communication and computing networks are not only critical infrastructures on their own, but underpin many other critical networks (e.g. energy, transport, finance, health …). In addition they are critically dependent on ICT technology. Therefore, the malfunctioning or disruption of the communication channel or of an IT system will have a cascading effect, on several other infrastructures or services that depend on it, potentially across all Europe.

This includes Industrial and Automation Control Systems (IACS). They are no longer isolated siloes but are fully integrated with corporate IT infrastructures. Despite this strong connection between the two infrastructures, there is only little awareness regarding IT risks that can affect IACS. An attack to IT assets can spread to the OT environment jumping to SCADA and Control Centres.

Many vulnerabilities of critical infrastructures, including the communication networks, stem from the fact that ICT systems are deployed in an environment or for an application that was not designed with security in mind. The deployment of ICT in new critical systems, including new generation ICT system, is exacerbating the problem by constantly introducing new risks and vulnerabilities, in particular for an interconnected system.

Scope:

Proposals should investigate the dependencies on communication networks and ICT components (including SCADA and IACS systems) of critical infrastructures, analyze and propose mitigation strategies and methodologies for assessing criticalities of services and detecting anomalies, developing tools and processes to simulate or monitor cascading effects due to ICT incidents, and develop self-healing mechanisms. ICT should be protected or re-designed at the software level, but also at the physical level, leading to more robust, resilient and survivable ICT infrastructure.



Disaster-resilience: safeguarding and securing society, including adapting to climate change

H2020-DRS-2015 — Sub call of: H2020-DRS-2014-2015

Planned Opening Date	25-03-2015		
Publication date	11-12-2013	**Deadline Date**	27-08-2015 17:00:00 (Brussels local time)
Total Call Budget	€93,070,000	**Main Pillar**	Societal Challenges
Status	Forthcoming	**OJ reference**	OJ C361/9 of 11 December 2013

Topic: **Critical Infrastructure Protection topic 3: Critical Infrastructure resilience indicator - analysis and development of methods for assessing resilience** **DRS-14-2015**

Specific challenge:

A better understanding of critical infrastructure architecture is necessary for defining measures to achieve a better resilience against threats in an integrated manner including natural and human threats/events (e.g. due to human errors or terrorist/criminal attacks).

Scope:

A holistic approach to the resilience of critical infrastructure should be followed, addressing a broad variety of issues including: human factors (i.e. safety issues radicalization), security, geo-politics, sociology, economy, etc. and increased vulnerability due to changing threats.

Disaster-resilience: safeguarding and securing society, including adapting to climate change

H2020-DRS-2015 — Sub call of: H2020-DRS-2014-2015

Planned Opening Date	25-03-2015		
Publication date	11-12-2013	**Deadline Date**	27-08-2015 17:00:00 (Brussels local time)
Total Call Budget	€93,070,000	**Main Pillar**	Societal Challenges
Status	Forthcoming	**OJ reference**	OJ C361/9 of 11 December 2013

Topic: **Critical Infrastructure Protection topic 1: Critical Infrastructure "smart grid" protection and resilience under "smart meters" threats** **DRS-12-2015**

Specific Challenge:

Critical Infrastructure functions are technologically and operationally interconnected, of which their exact possibilities and potential risks need to be better understood. For example: in the case of energy distribution networks, especially “smart grids”, the massive proliferation of "Smart Meters" as mandated by the Third energy Package introduces new threats. The same is applicable to all utility supply networks (e.g. water or gas system supply). The systems and meters of the charge points for electrical cars should be also a concern, specially considering the increasing market for this type of vehicles

Scope:

The objective is to analyse potential new threats generated by the massive introduction of “smart meters” on the distribution grid system and propose concrete solutions in order to mitigate the risks, guarantee the electromagnetic compatibility, improve resilience and reduce vulnerability of critical infrastructure “smart grid”, due for example to cyber-attacks, or to the locally diffused interconnectivity with renewable utility grids, and the existence of widely spread entry points that could locally influence the utility grid and its functioning, etc.

7 Targets and indicators

In order to check if the dissemination plan has been successful, the following indicators can be used:

- Number of references in technical journals;
- Number of hits on the website and tracking of the activity using statistics provided by the host;
- Interest in the service during the demonstration events.

After 18 months, the activity on the website is summarised in table below:

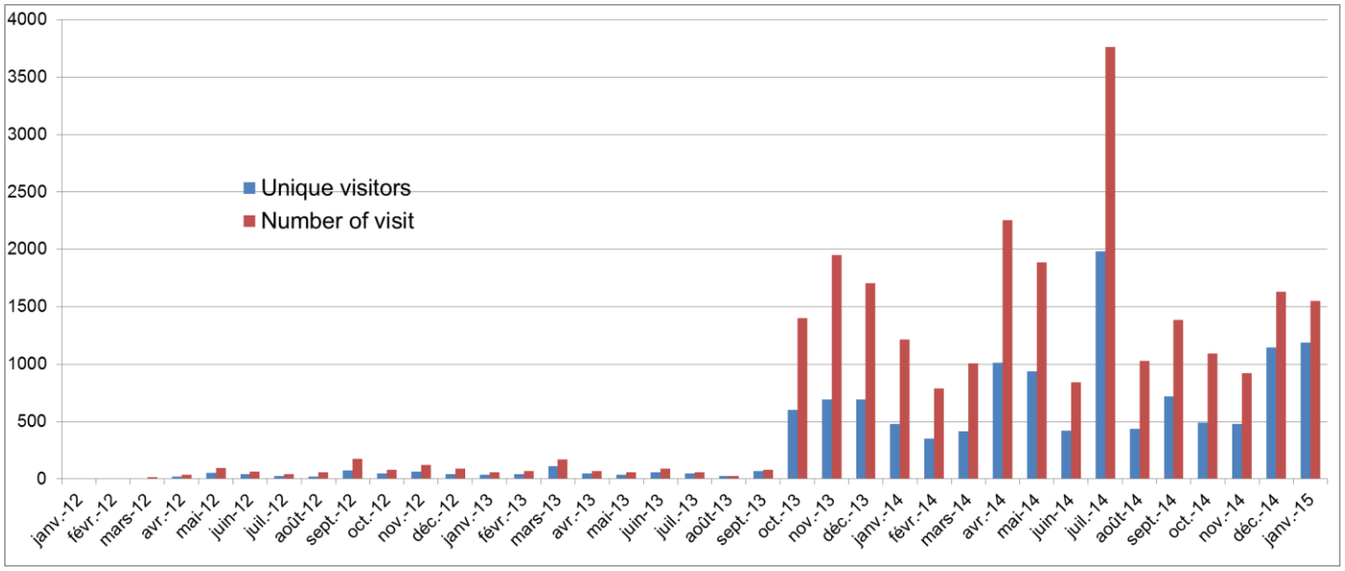


Figure 19: Visit on CockpitCi website

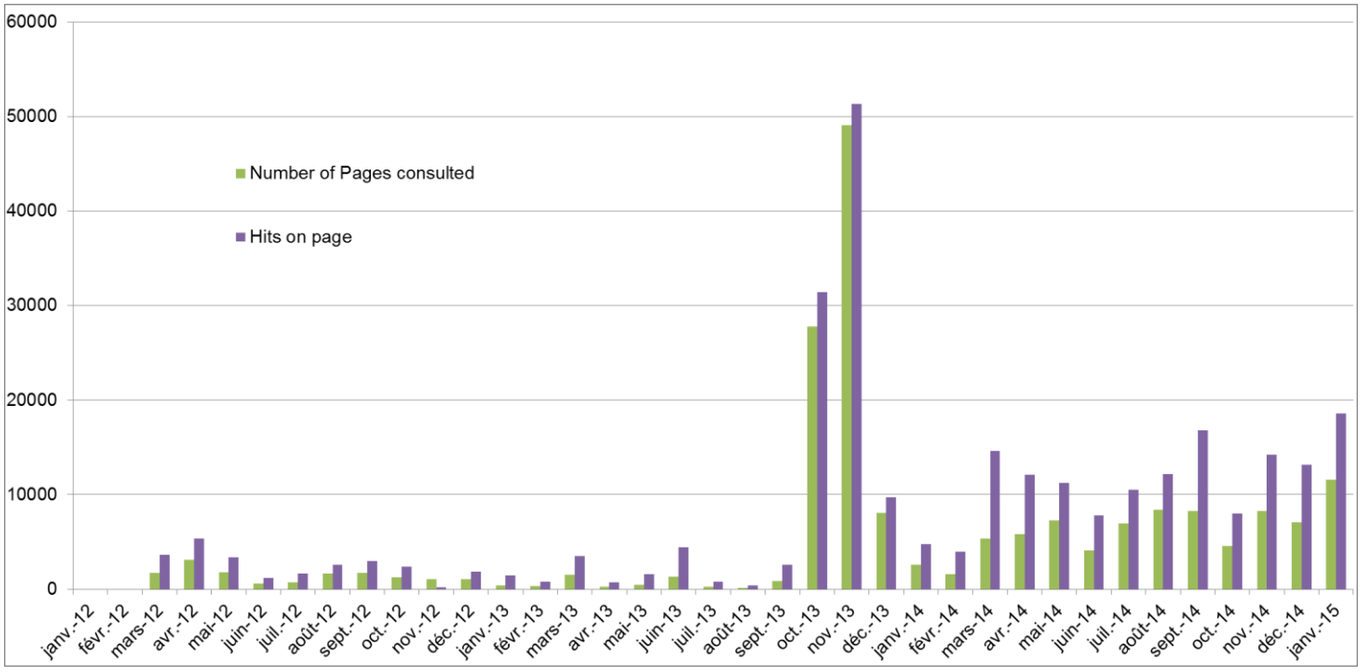


Figure 20: Hits on pages

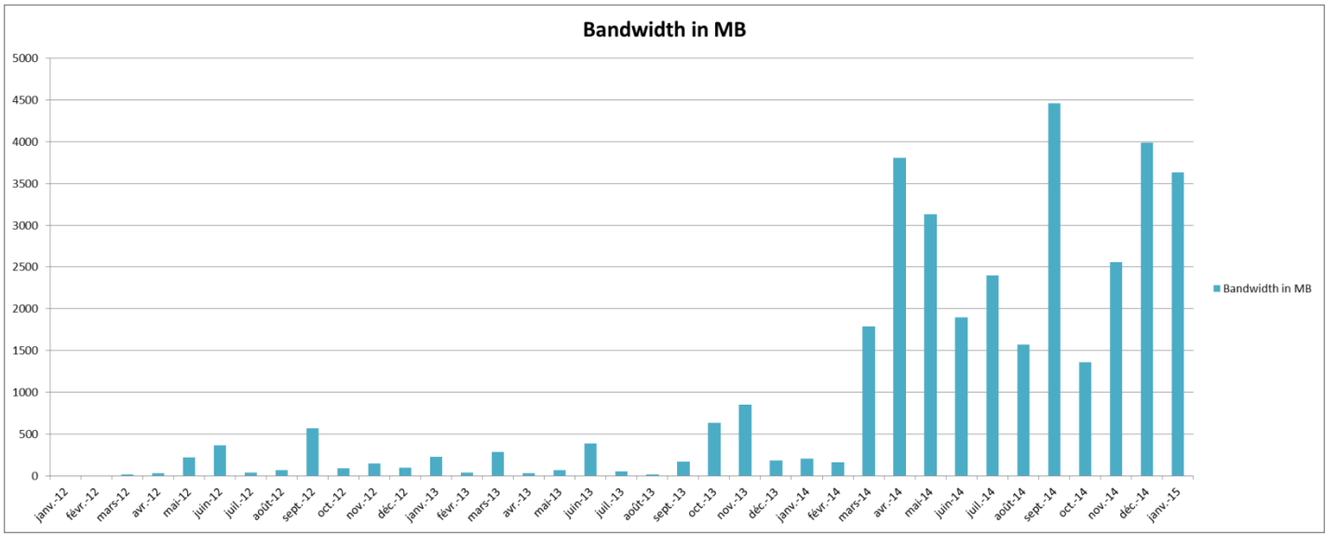


Figure 21: Use of web site bandwidth

Note: the important amount of hits during the October and November 2013 comes from a botnet attacks on blog comments. The problem has been fixed at the end of November.

According to this figure, the web site has been mainly visited after the main dissemination events: Cigre Congress (Mars 2014) and last three workshops, which deals with the dissemination strategy fixed by the consortium at start of the project.

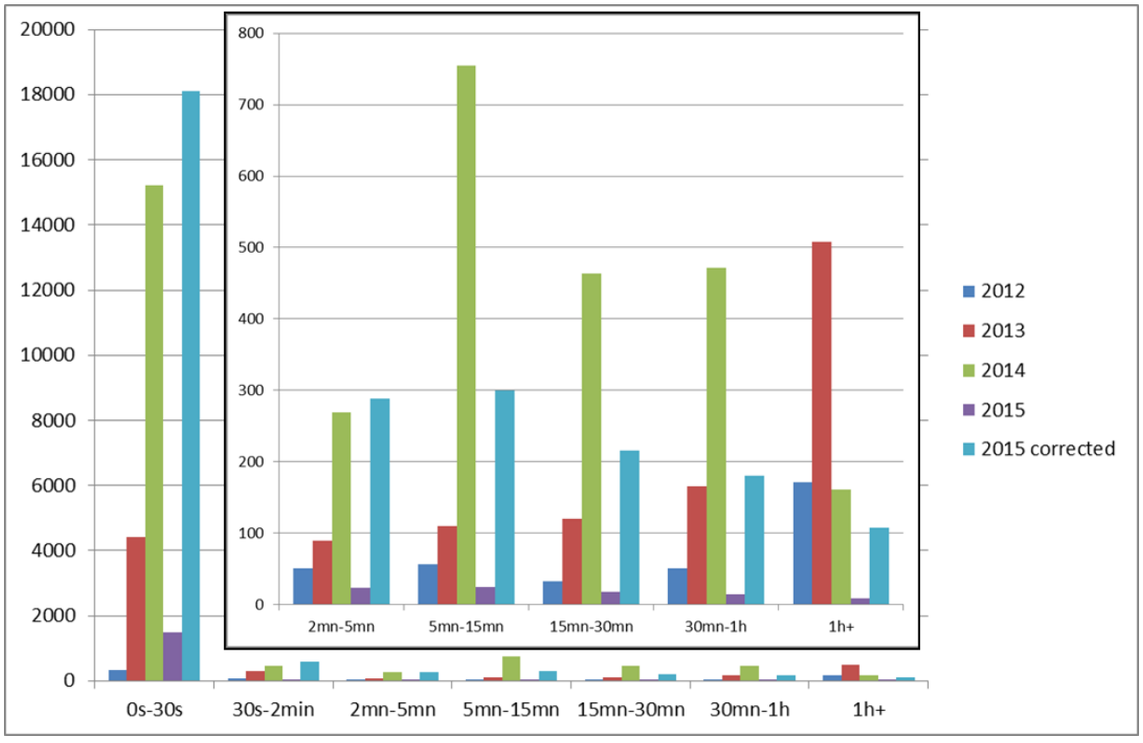


Figure 22: Time of visit to the CockpitCI website

According to the figure above (and excluding the very short visit which always remains the most important number of visit), we can consider that the website have been studied by the visitor (most important number between 15min and 1 hour).

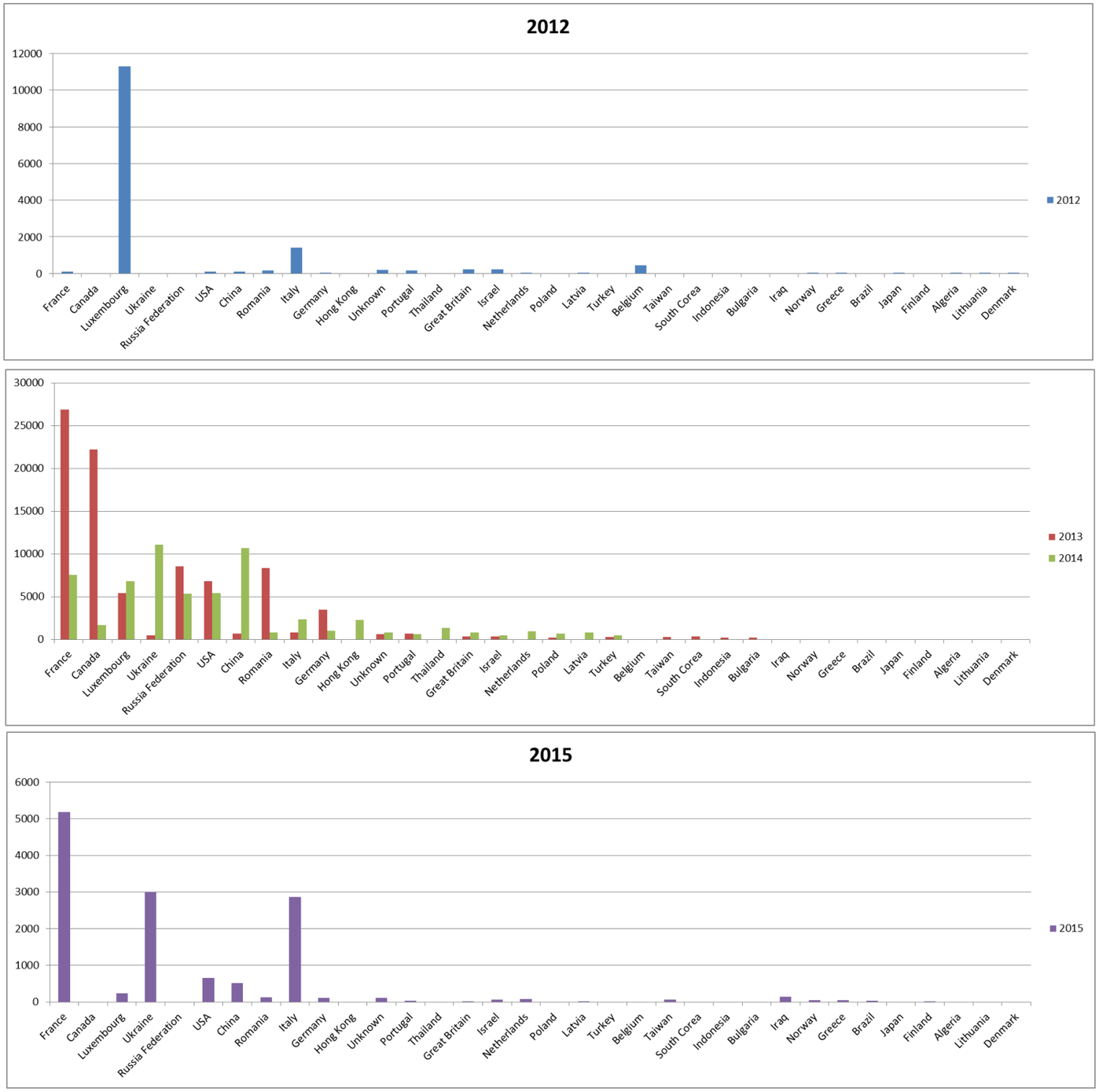


Figure 23: Geographical repartition of CockpitCI visitor

Note: At the beginning of the project website, it is normal that the most important visitor comes from Luxembourg as the total amount of visit is mainly due to the web-site set-up and test.

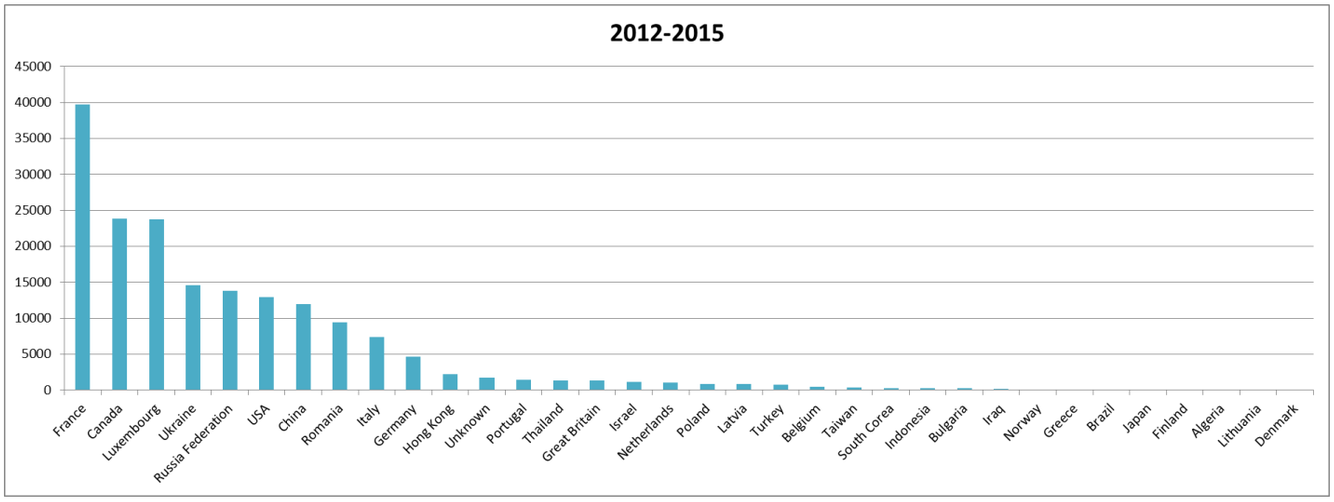


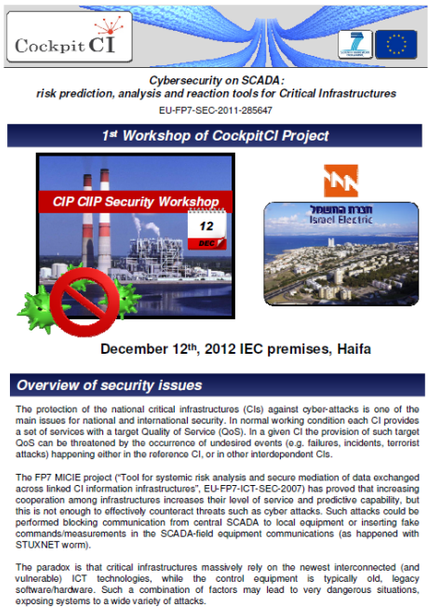
Figure 24: Summary of the geographical repartition for the 3 years

We can note that the web-site has been visited not only by European Countries but also by USA/CANADA and Russia and China, which can be considered as a really good point from a dissemination point of view and which can be linked with other dissemination action as workshop or attendance to International conference.

8 Annex A

8.1 Workshop in Israel

The following illustration is a facsimile of the workshop invitation given to interested parties and available on the CockpitCI website.



Cockpit CI

Cybersecurity on SCADA:
risk prediction, analysis and reaction tools for Critical Infrastructures

EU-FP7-SEC-2011-285647

1st Workshop of CockpitCI Project

CIP CIIP Security Workshop

Israel Electric

December 12th, 2012 IEC premises, Haifa

Overview of security issues

The protection of the national critical infrastructures (CIs) against cyber-attacks is one of the main issues for national and international security. In normal working condition each CI provides a set of services with a target Quality of Service (QoS). In a given CI the provision of such target QoS can be threatened by the occurrence of undesired events (e.g. failures, incidents, terrorist attacks) happening either in the reference CI, or in other interdependent CIs.

The FP7 MICIE project ("Tool for systemic risk analysis and secure mediation of data exchanged across linked CI information infrastructures", EU-FP7-ICT-SEC-2007) has proved that increasing cooperation among infrastructures increases their level of service and predictive capability, but this is not enough to effectively counteract threats such as cyber attacks. Such attacks could be performed blocking communication from central SCADA to local equipment or inserting fake commands/measurements in the SCADA-field equipment communications (as happened with STUXNET worm).

The paradox is that critical infrastructures massively rely on the newest interconnected (and vulnerable) ICT technologies, while the control equipment is typically old, legacy software/hardware. Such a combination of factors may lead to very dangerous situations, exposing systems to a wide variety of attacks.

Cockpit CI

CockpitCI Purpose

For years the world of Industrial Control Systems for CI has proceeded mostly on its own path, lagging behind the advances in information technology and cyber-security practices. This is no more acceptable and there is the need to complement business awareness with cyber awareness to reach an increased level of awareness (global awareness). CI operators ultimately demand for achieving a better awareness of the status of their CI in the System of Systems environment, in order to be able to take timely and aware decisions of intervention and this resulting into greater business continuity.

The CockpitCI project aims on one hand to continue the work done in MICIE by refining and updating the on-line Risk Predictor deployed in the SCADA centre and sharing real-time information among CI owners, on the other hand to add cyber detection capabilities in order to get a broader perspective in terms of security, to identify in near real time the CI functionalities impacted by cyber-attacks and to assess the degradation of CI delivered services.

CockpitCI aims to classify the associated risk level and activate a strategy of containment of the possible consequences of cyber-attacks together with the provision of some kind of intelligence to field equipment, allowing it to perform local decisions in order to self-identify and self-react to abnormal situations induced by cyber attacks.

Information

Project Website: www.cockpitci.eu
Coordinator Contact: Antonio Graziano
SELEX Sistemi Integrati S.p.A, Italy
agraziano@selex-si.com

Participants:

SELEX-SI: SELEX Sistemi Integrati S.p.A. IT
CRPHT: Centre de Recherche Public Henri Tudor – LU
CRAT: Consorzio per la Ricerca nell'Automatica e nelle Telecomunicazioni – IT
ROMA Tre: Dipartimento Informatica e Automazione, Università di Roma Tre – IT
ENEA: Agenzia nazionale per le nuove tecnologie, l'energia e lo sviluppo economico sostenibile – IT
IEC: Israel Electric Corp – IL
itrust consulting s.à.r.l. – LU
Multitel asbl – BE
University of Coimbra – PT
University of Surrey – UK
Transelectrica: Compania Nationala de Transport al energiei Electrice Transelectrica SA – RO
Lyse: Lyse Energi AS – NO

Cockpit CI

Workshop Objective

The objective of the workshop is to have an **open confrontation** on the issues addressed by the CockpitCI project with End Users and System Manufacturers in the Energy, ICT and Control Systems sectors.

Workshop Agenda 11:45 - 17:30

11:45 - 12:20	Registration
12:20 - 12:30	**IEC Welcome (Y. Shneck, IEC VP and CIO)**
12:30– 12:40	**IEC involvement in FP7 program (N. Trinczer, IEC Deputy VP)**
12:40 - 13:00	**Welcome (M. Shaton, Israel-Europe R&D Directorate General Manager)**
13:00 – 13:40	**Building Your Security Strategy in a Vulnerable World (A. Bar Lev, Check Point President, Israel)**
13:40 – 14:00	**SCADA Systems Cyber Security Challenges of European Utilities (A. Kvinnesland, Lyse IT Security Advisor, Norway)**
14:00 – 14:30	Coffee Break
14:30 – 16:30	**CockpitCI project presentation**

- Project overview (SELEX-SI, Italy)
- Modelling Industrial Control Systems under cyber attacks (ENEA, Italy)
- The problem of detecting cyber attacks in SCADA systems (University of Coimbra, Portugal)
- Cyber-physical risk prediction (Roma3, Italy)
- Hybrid test bed for Industrial Control Systems of Critical Infrastructures (IEC, Israel)
- Dissemination and exploitation (itrust, Luxemburg)

16:30 – 17:00	Coffee Break
17:00 – 17:30	**Panel: Discussions and Conclusions**

8.2 Workshop in Portugal

The following illustration is a facsimile of the workshop invitation given to interested parties and which was available on the CockpitCI website.

Cockpit CI

INVITATION TO THE 2ND WORKSHOP OF THE COCKPIT PROJECT

EU-FP7-SEC-2011-285647

CockpitCI
Cyber security on SCADA: risk prediction, analysis and reaction tools for Critical Infrastructures

Wednesday, March 20th, 2013
Departamento de Engenharia Informática
Pólo II da Universidade de Coimbra
3030-290 Coimbra, Portugal

GENERAL

The protection of the national critical infrastructures (CI) against cyber-attacks is one of the main issues for national and international security. In normal working condition each CI provides a set of services with a target Quality of Service (QoS). In a given CI the provision of such target QoS can be threatened by the occurrence of undesired events (e.g. failures, incidents, terrorist attacks) happening either in the reference CI, or in other interdependent CIs.

Previous European projects have proved that increasing cooperation among infrastructures increases their level of service and predictive capability, but this is not enough to effectively counteract threats such as cyber attacks. Such attacks could be performed blocking communication from central SCADA to local equipment or inserting fake commands or measurements in the SCADA-field equipment communications (as happened with STUXNET).

The paradox is that critical infrastructures massively rely on the newest interconnected (and vulnerable) ICT technologies, while the control equipment is typically old, legacy software and hardware. Such a combination of factors may lead to very dangerous situations, exposing systems to a wide variety of attacks.

COCKPITCI PURPOSE

For years the world of Industrial Control Systems for CI has proceeded mostly on its own path, lagging behind the advances in information technology and cyber-security practices. This is no more acceptable and there is the need to complement business awareness with cyber awareness to reach an increased level of awareness (global awareness). CI operators ultimately demand for achieving a better awareness of the status of their CI in the System of Systems environment, in order to be able to take timely and aware decisions of intervention and this resulting into greater business continuity.

The CockpitCI project aims on one hand to continue the work done in previous European projects, such as FP7 MICIE, by refining and updating the on-line Risk Predictor deployed in the SCADA center and sharing real-time information among CI owners, on the other hand to add cyber detection capabilities in order to get a broader perspective in terms of security, to identify in near real time the CI functionalities impacted by cyber-attacks and to assess the degradation of CI delivered services.

CockpitCI aims to classify the associated risk level and activate a strategy of containment of the possible consequences of cyber-attacks together with the provision of some kind of intelligence to field equipment, allowing it to perform local decisions in order to self-identify and self-react to abnormal situations induced by cyber attacks.

WORKSHOP OBJECTIVES

The objective of the workshop is to have an open confrontation on the issues addressed by the CockpitCI project with End Users and System Manufacturers in the Energy, ICT and Control Systems sectors. In the first part of the workshop, the CockpitCI concept will be presented. Next, selected invited presentations industry stakeholders will provide an overview of current industry needs and practices. The workshop will finish with a joint discussion panel.

Cockpit CI

MORE INFORMATION

Project Website:
www.CockpitCI.eu
Coordinator contact:
Antonio Graziano
SELEX Sistemi Integrati S.p.A., Italy
agraziano@selex-si.com

PARTICIPANTS

› SELEX Sistemi Integrati S.p.A., IT
› Centre de Recherche Public Henri Tudor, LU
› CRAT – "Sapienza" University of Rome, IT
› Università di Roma Tre, IT
› ENEA, IT
› Israel Electric Corp, IL
› itrust consulting s.à r.l., LU
› Multitel asbl, BE
› University of Coimbra, PT
› University of Surrey, UK
› Transelectrica SA, RO
› Lyse Energi AS, NO

WORKSHOP AGENDA (14:00 – 18:00)

14:00 – 14:10: Welcome and Introduction
- *Paulo Simões and Antonio Graziano*

14:10 – 15:30: The CockpitCI Approach to Cyber Security
Session Chair: *Leonid Lev, Israel Electric Corporation*
- CockpitCI project overview
  Antonio Graziano, SELEX Sistemi Integrati S.p.A.
- Scenario and models of SCADA and ICS under cyber attacks
  Michele Minichino, ENEA
- Smart detection strategy
  Tiago Cruz, University of Coimbra
- Cyber-risk prediction strategy
  Stefano Panzieri, Università di Roma Tre

15:30 – 16:00: Coffee-Break

16:00 – 17:30: Industry Perspectives
Session Chair: *Miguel Martins, itrust consulting*
- Cybersecurity in Electricity Distribution
  Nuno Pereira, EDP
- FeedZai Pulse: Uncover and Manage Anomalies in Real-Time
  Paulo Marques, FeedZai
- CECRIS – CErtification of CRItical Systems
  Marco Vieira, University of Coimbra
- Energy Metering
  Ricardo Clérigo, ISA – Intelligent Sensing Anywhere

17:30 – 18:00: Panel Discussion
- Towards Safer Critical Infrastructures
  Antonio Graziano, Marco Vieira, Michele Minichino, Nuno Pereira, Paulo Marques, Ricardo Clérigo, Stefano Panzieri, Tiago Cruz

18:00 Wrap-up and Closing

Cockpit CI

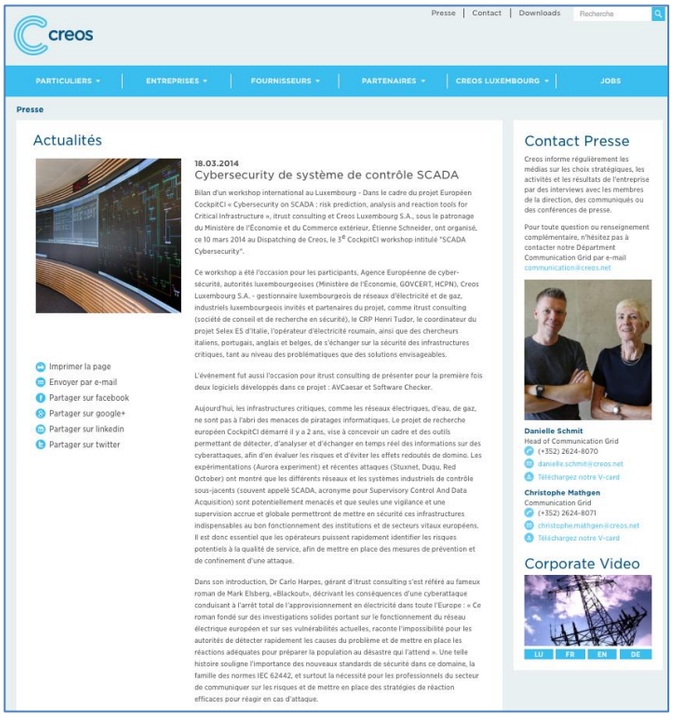
Facsimile of the Workshop Invitation

8.3 Luxembourg Workshop

The following illustration is a facsimile of the workshop invitation given to interested parties and which was available on the CockpitCI website.

Facsimile of the Workshop Invitation

The following pictures are the facsimiles of the web-news reporting the Luxembourg events:



8.4 Bucharest Workshop

The following illustration is a facsimile of the workshop invitation given to interested parties and which was available on the CockpitCI website.

Facsimile of the Workshop Invitation

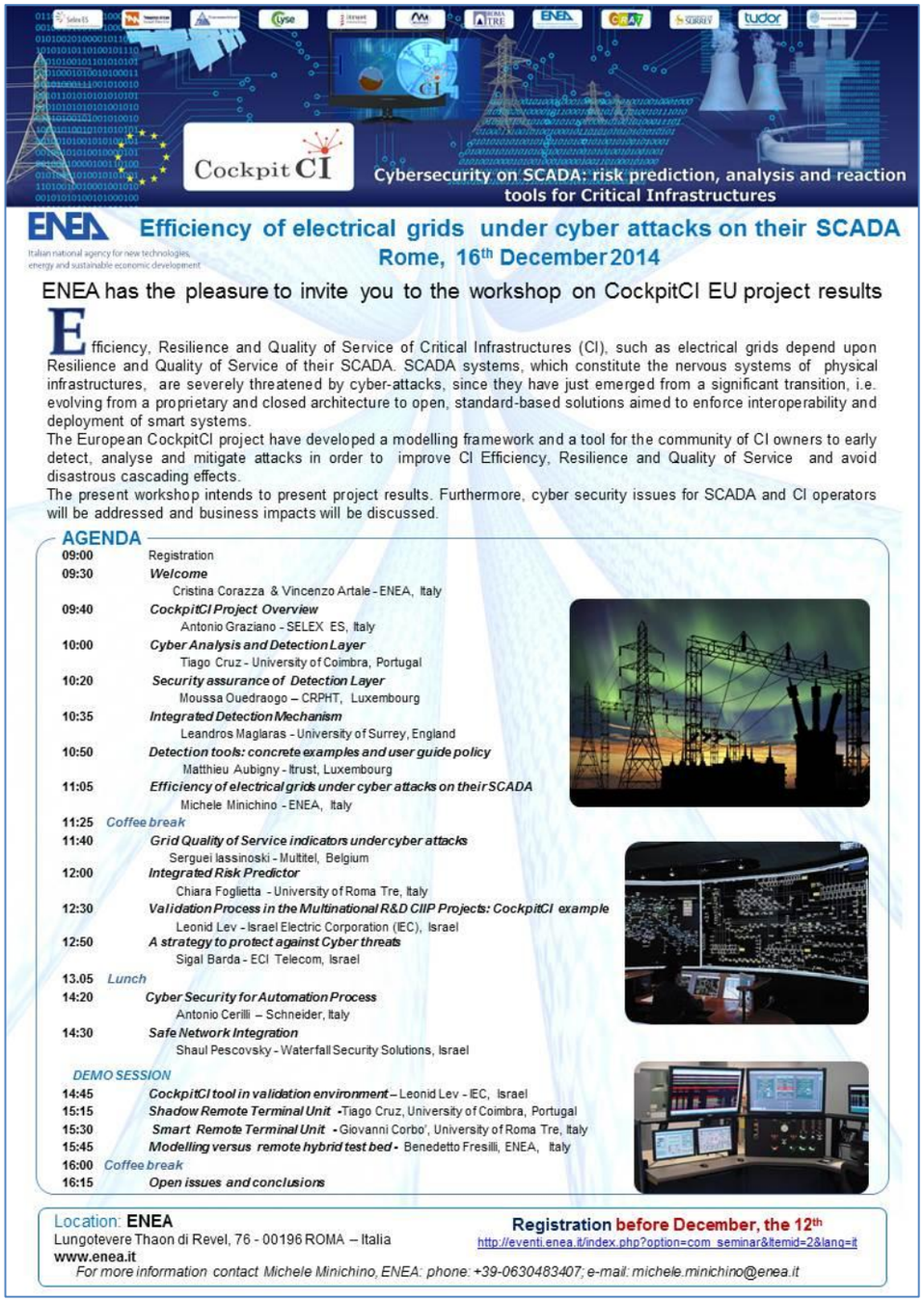
8.5 Stavanger Workshop

The following illustration is a facsimile of the workshop invitation given to interested parties and which was available on the CockpitCI website.

Facsimile of the Workshop Invitation

8.6 Roma Workshop

The following illustration is a facsimile of the workshop invitation given to interested parties and which was available on the CockpitCI website.



Facsimile of the Workshop Invitation

The following pictures are the facsimile of press release reporting the Roma event:

COMUNICATI STAMPA

Energia: progetto ENEA per rafforzare sicurezza reti
In collaborazione con Selex (Finmeccanica) e partner europei e israeliani

Rafforzare la sicurezza e la capacità di risposta delle infrastrutture di rete alle criticità provocate da eventi naturali, da guasti, errori umani, ma anche cyber attacchi. E' l'obiettivo al quale sta lavorando l'ENEA con alcuni gestori di rete europei, il TSO norvegese Lyse, istituti di ricerca e universita straniere e operatori delle reti elettriche, idriche e delle tlc di Israele. Per l'Italia il partner è la SELEX del Gruppo Finmeccanica.

I risultati ottenuti ad oggi per rendere disponibile ai gestori di infrastrutture 'critiche' – come reti elettriche, del gas o di tlc- ma anche delle amministrazioni locali e la Protezione civile un DSS, Decision support system, ovvero un sistema di monitoraggio continuo e di supporto alle decisioni in caso di crisi, sono stati presentati in un workshop all'ENEA a Roma al quale hanno partecipato esperti delle Università di Coimbra, del Surrey, di Roma Tre.

"A fronte di evento naturale avverso, di guasti o anche di attacchi informatici, il buon funzionamento e la capacità di gestione dell'evento sono fondamentali per non mandare in tilt tutto il sistema. Inoltre, l'ingente produzione da fonti rinnovabili e l'evoluzione verso le smart grids rendono più 'vulnerabile' il sistema. Da qui –spiega il ricercatore ENEA Michele Minichino- l'importanza di sistemi avanzati per ridurre i rischi e ottimizzare l'efficienza delle reti e degli SCADA (Supervision And Data Acquisition) che sono il 'sistema nervoso' delle infrastrutture''. Nello specifico, l'ENEA sta realizzando un centro di simulazione distribuito tra la Casaccia, Palermo e Bari dove sarà possibile rappresentare ed eseguire scenari di pianificazione e di esercizio di reti elettriche attive (con generazione distribuita e sistemi di accumulo), rete idrica, rete del gas.

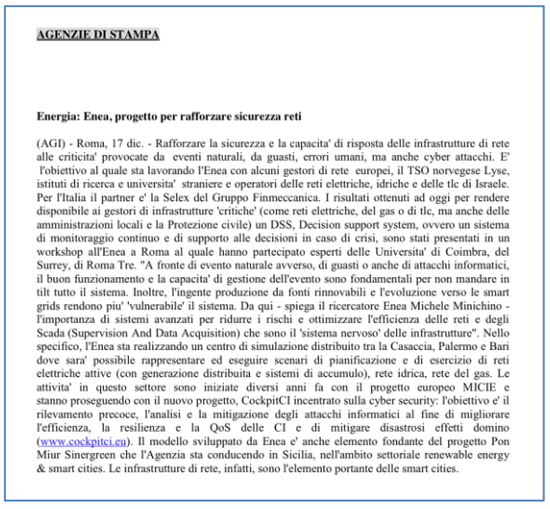
Le attività in questo settore sono iniziate diversi anni fa con il progetto europeo MICIE e stanno proseguendo con il nuovo progetto, CockpitCI incentrato sulla cyber security: l'obiettivo è il rilevamento precoce, l'analisi e la mitigazione degli attacchi informatici al fine di migliorare l'efficienza, la resilienza e la QoS delle CI e di mitigare disastrosi effetti domino (www.cockpitci.eu).
Il modello sviluppato da ENEA è anche elemento fondante del progetto PON MIUR SINERGREEN (http://sinergreen.cdc.unict.it/index.php/it/) che l'Agenzia sta conducendo in Sicilia, nell'ambito settoriale renewable energy & smart cities. Le infrastrutture di rete, infatti, sono l'elemento portante delle smart cities.

Per ulteriori informazioni vedi il video realizzato dalla WebTv ENEA al seguente link:

Progetto CockpitCI, per l'efficienza e la sicurezza delle reti elettriche

http://webtv.enea.it/Members/webtvadmin/videos/cockpitcifinal.mpg

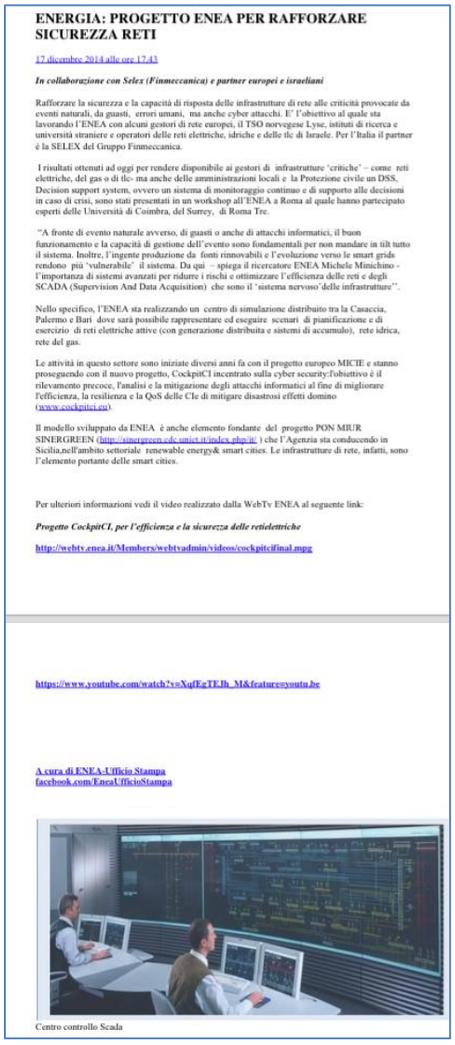
https://www.youtube.com/watch?v=XqfEgTEJh_M&feature=youtu.be



AGENZIE DI STAMPA

Energia: Enea, progetto per rafforzare sicurezza reti

(AGI) - Roma, 17 dic. - Rafforzare la sicurezza e la capacita' di risposta delle infrastrutture di rete alle criticita' provocate da eventi naturali, da guasti, errori umani, ma anche cyber attacchi. E' l'obiettivo al quale sta lavorando l'Enea con alcuni gestori di rete europei, il TSO norvegese Lyse, istituti di ricerca e universita' straniere e operatori delle reti elettriche, idriche e delle tlc di Israele. Per l'Italia il partner e' la Selex del Gruppo Finmeccanica. I risultati ottenuti ad oggi per rendere disponibile ai gestori di infrastrutture 'critiche' (come reti elettriche, del gas o di tlc, ma anche delle amministrazioni locali e la Protezione civile) un DSS, Decision support system, ovvero un sistema di monitoraggio continuo e di supporto alle decisioni in caso di crisi, sono stati presentati in un workshop all'Enea a Roma al quale hanno partecipato esperti delle Universita' di Coimbra, del Surrey, di Roma Tre. "A fronte di evento naturale avverso, di guasti o anche di attacchi informatici, il buon funzionamento e la capacita' di gestione dell'evento sono fondamentali per non mandare in tilt tutto il sistema. Inoltre, l'ingente produzione da fonti rinnovabili e l'evoluzione verso le smart grids rendono piu' 'vulnerabile' il sistema. Da qui - spiega il ricercatore Enea Michele Minichino - l'importanza di sistemi avanzati per ridurre i rischi e ottimizzare l'efficienza delle reti e degli Scada (Supervision And Data Acquisition) che sono il 'sistema nervoso' delle infrastrutture". Nello specifico, l'Enea sta realizzando un centro di simulazione distribuito tra la Casaccia, Palermo e Bari dove sara' possibile rappresentare ed eseguire scenari di pianificazione e di esercizio di reti elettriche attive (con generazione distribuita e sistemi di accumulo), rete idrica, rete del gas. Le attivita' in questo settore sono iniziate diversi anni fa con il progetto europeo MICIE e stanno proseguendo con il nuovo progetto, CockpitCI incentrato sulla cyber security: l'obiettivo e' il rilevamento precoce, l'analisi e la mitigazione degli attacchi informatici al fine di migliorare l'efficienza, la resilienza e la QoS delle CI e di mitigare disastrosi effetti domino (www.cockpitci.eu). Il modello sviluppato da Enea e' anche elemento fondante del progetto Pon Miur Sinergreen che l'Agenzia sta conducendo in Sicilia, nell'ambito settoriale renewable energy & smart cities. Le infrastrutture di rete, infatti, sono l'elemento portante delle smart cities.



ENERGIA: PROGETTO ENEA PER RAFFORZARE SICUREZZA RETI

17 dicembre 2014 alle ore 17.43

In collaborazione con Selex (Finmeccanica) e partner europei e israeliani

Rafforzare la sicurezza e la capacità di risposta delle infrastrutture di rete alle criticità provocate da eventi naturali, da guasti, errori umani, ma anche cyber attacchi. E' l'obiettivo al quale sta lavorando l'ENEA con alcuni gestori di rete europei, il TSO norvegese Lyse, istituti di ricerca e universita straniere e operatori delle reti elettriche, idriche e delle tlc di Israele. Per l'Italia il partner è la SELEX del Gruppo Finmeccanica.

I risultati ottenuti ad oggi per rendere disponibile ai gestori di infrastrutture 'critiche' – come reti elettriche, del gas o di tlc- ma anche delle amministrazioni locali e la Protezione civile un DSS, Decision support system, ovvero un sistema di monitoraggio continuo e di supporto alle decisioni in caso di crisi, sono stati presentati in un workshop all'ENEA a Roma al quale hanno partecipato esperti delle Università di Coimbra, del Surrey, di Roma Tre.

"A fronte di evento naturale avverso, di guasti o anche di attacchi informatici, il buon funzionamento e la capacità di gestione dell'evento sono fondamentali per non mandare in tilt tutto il sistema. Inoltre, l'ingente produzione da fonti rinnovabili e l'evoluzione verso le smart grids rendono più 'vulnerabile' il sistema. Da qui – spiega il ricercatore ENEA Michele Minichino - l'importanza di sistemi avanzati per ridurre i rischi e ottimizzare l'efficienza delle reti e degli SCADA (Supervision And Data Acquisition) che sono il 'sistema nervoso' delle infrastrutture''.

Nello specifico, l'ENEA sta realizzando un centro di simulazione distribuito tra la Casaccia, Palermo e Bari dove sarà possibile rappresentare ed eseguire scenari di pianificazione e di esercizio di reti elettriche attive (con generazione distribuita e sistemi di accumulo), rete idrica, rete del gas.

Le attività in questo settore sono iniziate diversi anni fa con il progetto europeo MICIE e stanno proseguendo con il nuovo progetto, CockpitCI incentrato sulla cyber security:l'obiettivo è il rilevamento precoce, l'analisi e la mitigazione degli attacchi informatici al fine di migliorare l'efficienza, la resilienza e la QoS delle CIe di mitigare disastrosi effetti domino (www.cockpitci.eu).

Il modello sviluppato da ENEA è anche elemento fondante del progetto PON MIUR SINERGREEN (http://sinergreen.cdc.unict.it/index.php/it/) che l'Agenzia sta conducendo in Sicilia,nell'ambito settoriale renewable energy& smart cities. Le infrastrutture di rete, infatti, sono l'elemento portante delle smart cities.

Per ulteriori informazioni vedi il video realizzato dalla WebTv ENEA al seguente link:

Progetto CockpitCI, per l'efficienza e la sicurezza delle retielettriche

http://webtv.enea.it/Members/webtvadmin/videos/cockpitcifinal.mpg

https://www.youtube.com/watch?v=XqfEgTEJh_M&feature=youtu.be

A cura di ENEA-Ufficio Stampa
facebook.com/EneaUfficioStampa

Centro controllo Scada

ENEA Home Mailing list Per contattarci Cerca

Sei in: Home » Comunicati stampa » Energia: progetto ENEA per rafforzare sicurezza reti

COMUNICATI STAMPA
QUALCHE SPUNTO SU...
NEWS
EVENTI
RASSEGNA STAMPA
L'ENEA IN ONDA
ENEA WEB TV
TUTTI I NOSTRI FEED

COMUNICATI STAMPA

ENERGIA: PROGETTO ENEA PER RAFFORZARE SICUREZZA RETI
In collaborazione con Selex (Finmeccanica) e partner europei e israeliani

Rafforzare la sicurezza e la capacità di risposta delle infrastrutture di rete alle criticità provocate da eventi naturali, da guasti, errori umani, ma anche cyber attacchi. E' l'obiettivo al quale sta lavorando l'ENEA con alcuni gestori di rete europei, il TSO norvegese Lyse, istituti di ricerca e universita straniere e operatori delle reti elettriche, idriche e delle tlc di Israele. Per l'Italia il partner è la SELEX del Gruppo Finmeccanica.

I risultati ottenuti ad oggi per rendere disponibile ai gestori di infrastrutture 'critiche' - come reti elettriche, del gas o di tlc- ma anche delle amministrazioni locali e la Protezione civile un DSS, Decision support system, ovvero un sistema di monitoraggio continuo e di supporto alle decisioni in caso di crisi, sono stati presentati in un workshop all'ENEA a Roma al quale hanno partecipato esperti delle Università di Coimbra, del Surrey, di Roma Tre.

"A fronte di evento naturale avverso, di guasti o anche di attacchi informatici, il buon funzionamento e la capacità di gestione dell'evento sono fondamentali per non mandare in tilt tutto il sistema. Inoltre, l'ingente produzione da fonti rinnovabili e l'evoluzione verso le smart grids rendono più 'vulnerabile' il sistema. Da qui –spiega il ricercatore ENEA Michele Minichino- l'importanza di sistemi avanzati per ridurre i rischi e ottimizzare l'efficienza delle reti e degli SCADA (Supervision And Data Acquisition) che sono il 'sistema nervoso' delle infrastrutture''.
Nello specifico, l'ENEA sta realizzando un centro di simulazione distribuito tra la Casaccia, Palermo e Bari dove sarà possibile rappresentare ed eseguire scenari di pianificazione e di esercizio di reti elettriche attive (con generazione distribuita e sistemi di accumulo), rete idrica, rete del gas.

Le attività in questo settore sono iniziate diversi anni fa con il progetto europeo MICIE e stanno proseguendo con il nuovo progetto, CockpitCI incentrato sulla cyber security: l'obiettivo è il rilevamento precoce, l'analisi e la mitigazione degli attacchi informatici al fine di migliorare l'efficienza, la resilienza e la QoS delle CI e di mitigare disastrosi effetti domino (www.cockpitci.eu).
Il modello sviluppato da ENEA è anche elemento fondante del progetto PON MIUR SINERGREEN (http://sinergreen.cdc.unict.it/index.php/it/) che l'Agenzia sta conducendo in Sicilia, nell'ambito settoriale renewable energy & smart cities. Le infrastrutture di rete, infatti, sono l'elemento portante delle smart cities.

Per ulteriori informazioni vedi il video realizzato dalla WebTv ENEA al seguente link:

Progetto CockpitCI, per l'efficienza e la sicurezza delle reti elettriche

http://webtv.enea.it/Members/webtvadmin/videos/cockpitcifinal.mpg

18/12/2014 1

ia: progetto ENEA per rafforzare sicurezza reti http://titano.sede.enea.it/Stampa/skin2col.php?page=comunicatodetai

https://www.youtube.com/watch?v=XqfEgTEJh_M&feature=youtu.be

9 Annexe B: advertisement material

Posters and roller with some relevant results have been created for the Cigre Congress and used as advertisement material for every workshop from this date. Typically, poster sizes are A0 and A1.

Linked to a poster, flyers have been prepared in order to distribute to interested parties with a summary of the poster contents and the contacts of the consortium members. Various formats exist, but the most current flyer format is a trifold A4 sheet or twofold A4/A3 sheet.

Figure 25: CockpitCI project overview poster

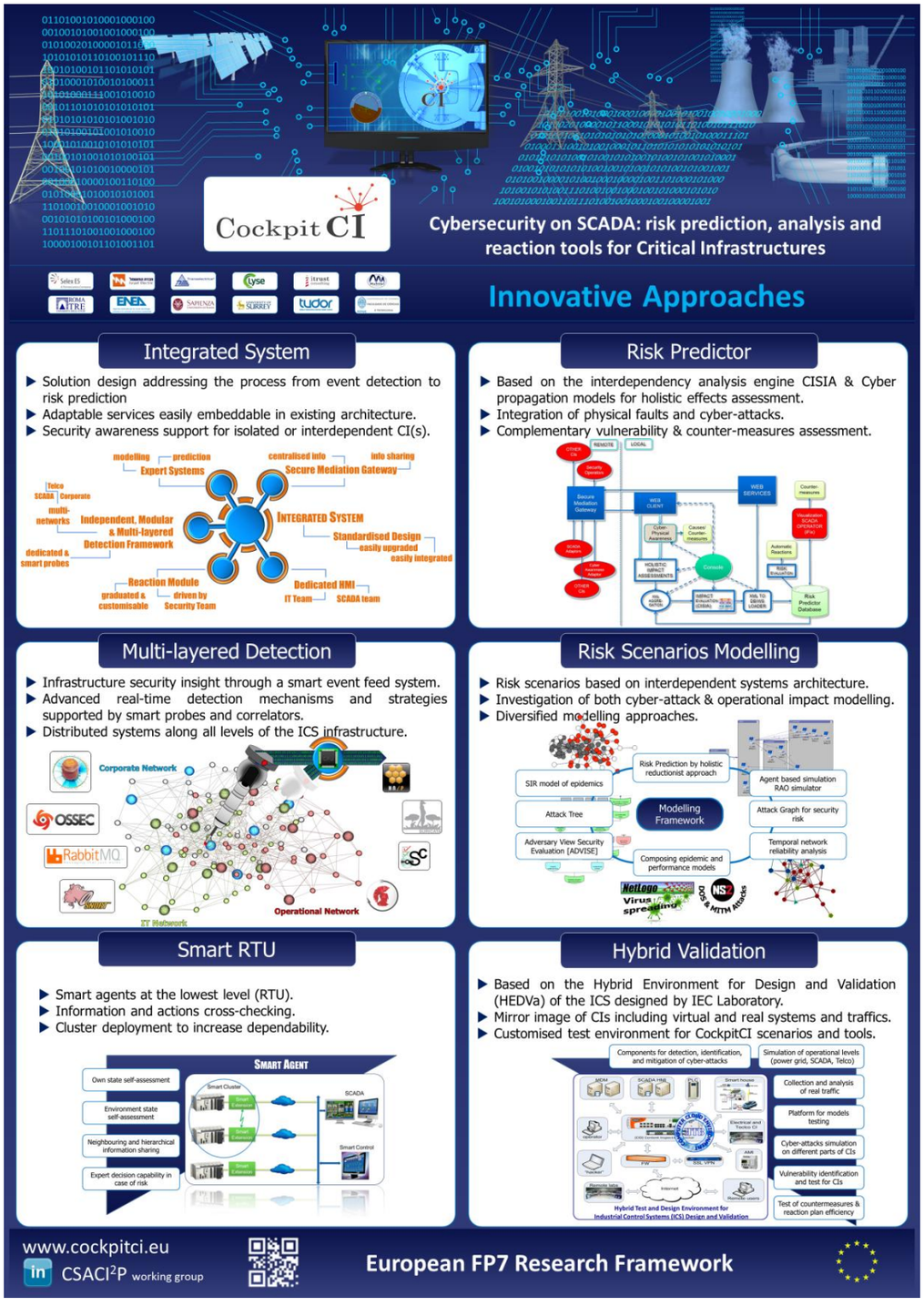
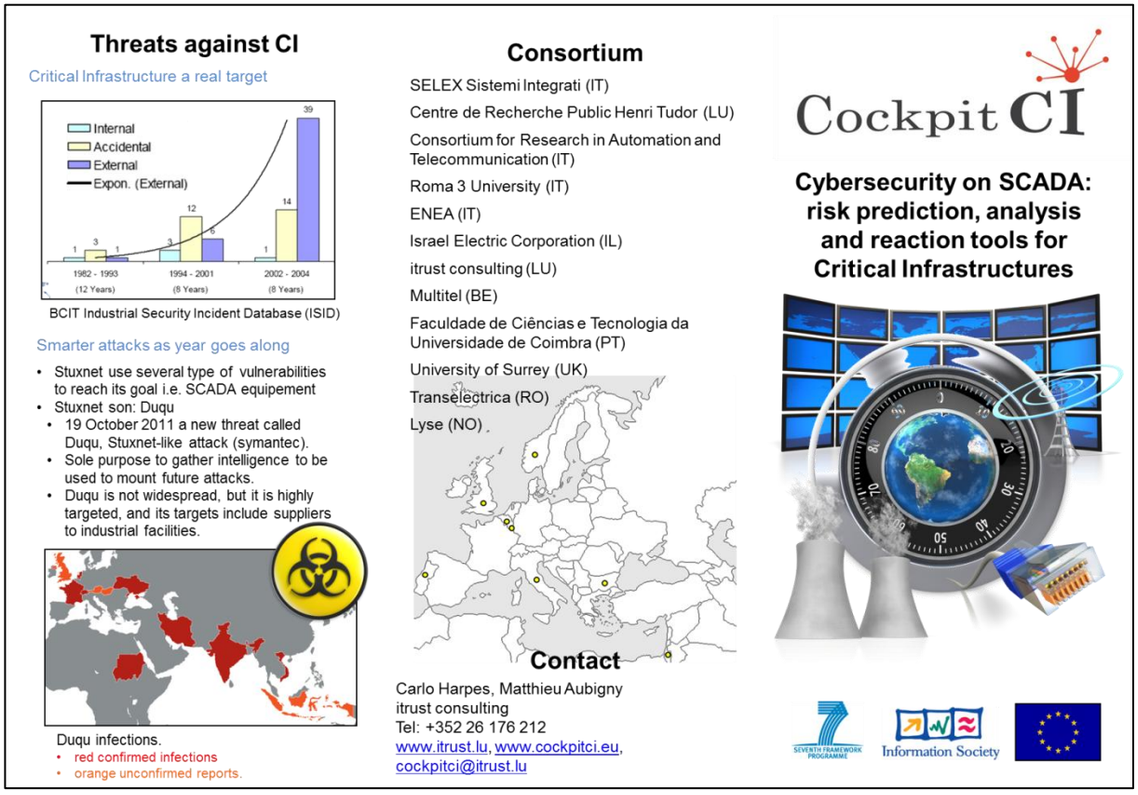


Figure 26: CockpitCI project innovations poster

Figure 27: CockpitCI project roller



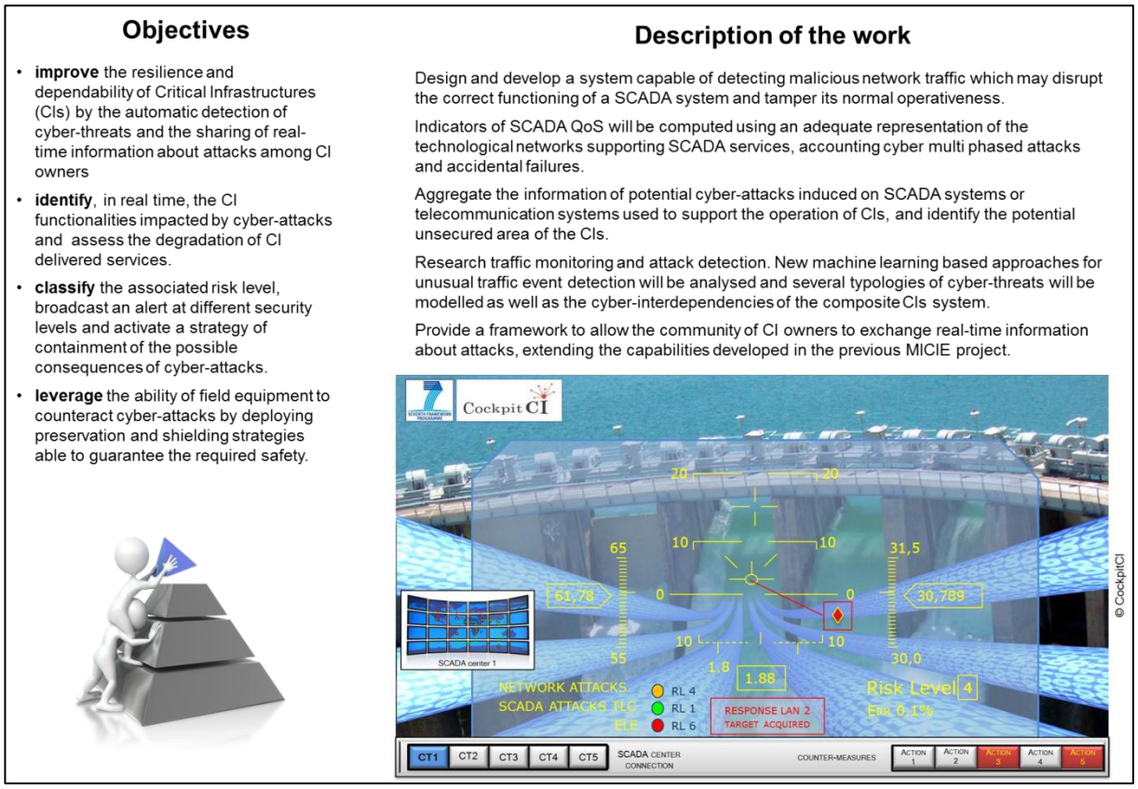
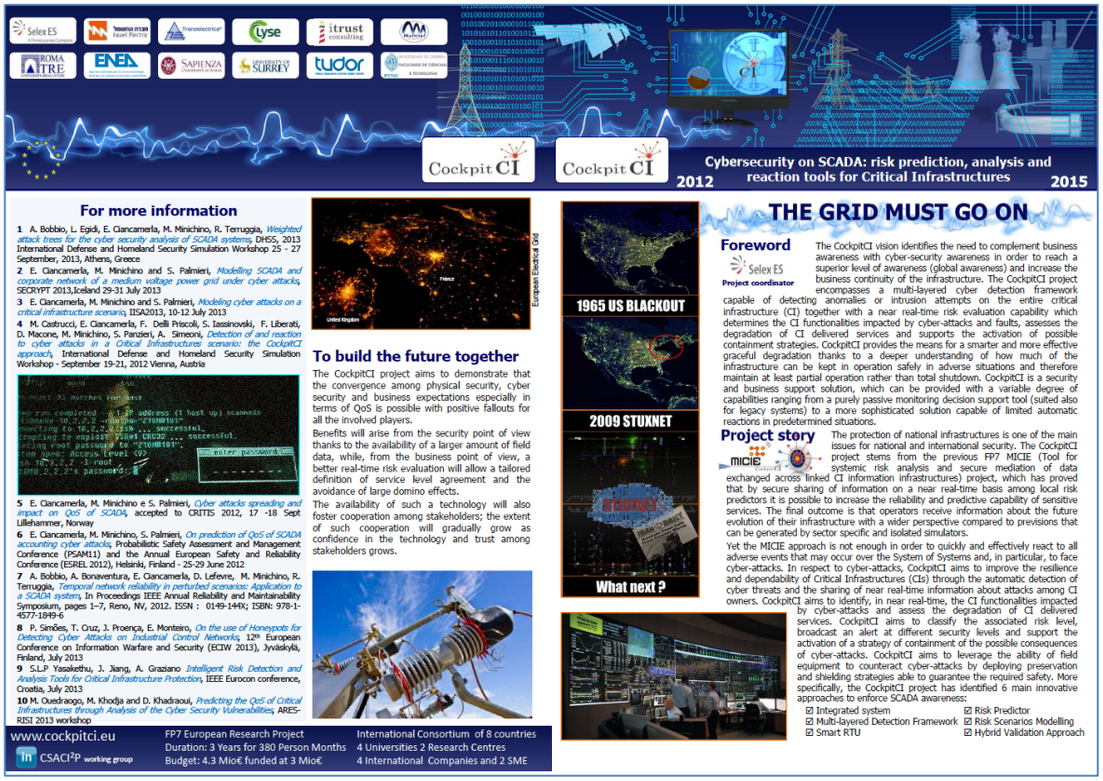


Figure 28: Flyer provided for the Berlin/Hamburg event



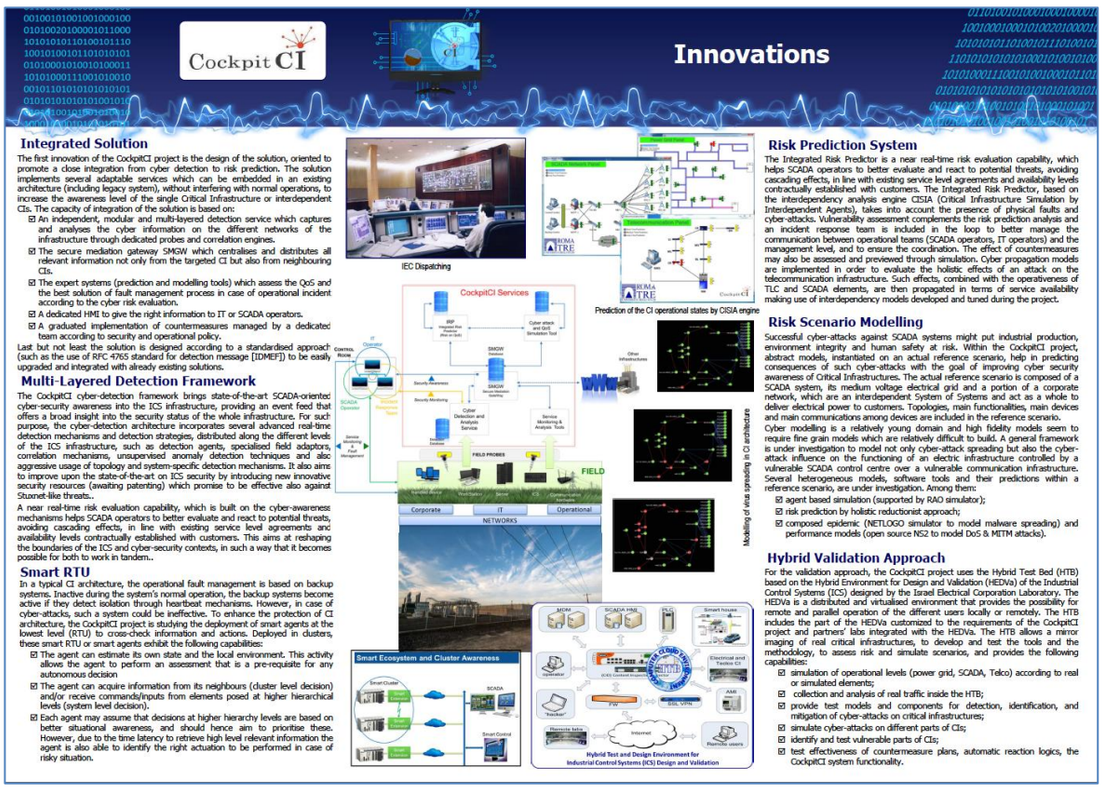


Figure 29: Flyer provided for the Cigre Congress and used from this date