Cockpit CI

SEVENTH FRAMEWORK PROGRAMME

FP7-SEC-2011-1 Project 285647

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

D5.1 – CockpitCI System requirements

General information	
Submission date	31/05/2012
Dissemination level	Public
State	Final Version
Work package	WP5000 - System Development and Integration
Task	Task 5001 - Functional and ICT System requirements
Delivery date	31/05/2012

Editors

Name	Organisation
Ricci Pietro	SELEX-SI

Authors

Name	Organisation
Antonio Graziano, Pietro Ricci, Riccardo Di Stefano, PierMaurizio Di Placido	SELEX-SI
Donato Macone, Francesco Liberati, Andrea Simeoni, Francesco Delli Priscoli. Roberto Cusani, Manlio Proia, Vincenzo Suraci and all the UoR-CRAT team	CRAT
Ester Ciancamerla, Michele Minichino	ENEA

Reviewers

Name	Organisation	Date
Stefano Panzieri	ROMA3	29/05/2012
Leonid Lev	IEC	30/05/2012

Table of contents

List of figures

List of table

1 Introduction

This document is the first deliverable of the CockpitCI project (Task 5001). Its objective is to define the main system requirements of the CockpitCI tool and act as a guideline for tasks to follow. In order to make a clear and contextual exposition of CockpitCI system requirements, in the following the motivations, the vision and the objectives of the CockpitCI project are briefly recalled.

The aim of the CockpitCI project is to provide an integrated set of solutions for dealing with protection of SCADA systems against cyber attacks. SCADA systems are computer-based control systems which are used to monitor and control a variety of industrial processes and operations, such as electricity and gas distribution, water treatment or railway transportation. These processes include also Critical Infrastructures (CI [1]), i.e. those assets (whether physical or virtual) that are so vital that their disruption would have a debilitating impact on security and prosperity of communities. One of the modern concepts to be considered when dealing with CIs protection is *interdependency*: CIs can no longer be modelled or analysed as isolated entities, because today they are part of a complex network (System of Systems) of physical and logical interactions. This makes the single CI vulnerable not only to internal failures or design deficiencies, or attacks taking place in the internal domain of the infrastructure, but also to external attacks, failures and threats conveyed along links with the environment. In this regard, the increasing dependency of the CI domain on advanced ICT solutions is giving rise to new sources of interdependencies, exposing CIs to new vulnerabilities and threats. Among them, cyber attacks and cyber-threats are of utmost concern.

In this perspective, the main objective of the CockpitCI project is to increase the resilience of SCADA systems (and therefore CIs) in presence of cyber attacks. The project intends to achieve this result by contributing to the following fields of CI protection research:

- Definition and development of a **heterogeneous (cross CI domain) modelling framework** for predicting the QoS delivered by SCADA systems (WP2000) in presence of cyber attacks;
- Definition of a **cyber-analysis and detection layer**, for early detection of cyber attacks (WP 3000);
- Definition of an **online risk prediction system**, enhancing global awareness and local sensing/reaction capabilities (WP4000);
- Definition of a **secure mediation network**, supporting secure and reliable exchange of data between linked CIs (WP 5000).

As it will also appear from the collection of end-user requirements presented later in the document, the CockpitCI project introduces significant innovations in each of these fields, in order to meet CI operators and stakeholders' expectations. As a matter of fact, and also as the lessons learned from recent cyber attack events (e.g. STUXNET, SLAMMER, etc.) and from the outcome of recent research projects (e.g. FP6 SAFEGUARD, FP7 CRUTIAL, FP7 MICIE, etc.) clearly indicate, 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 (resulting into greater business continuity).

The CockpitCI project will make a step in this direction, by merging and composing the "local vision" provided by information collected from the field equipment, with the global one at CI-level which collates the remote information about the state of linked (*interdependent*) CIs. Intelligence will be added and integrated at different levels of the system, starting from the field, where a **smart layer of detection agents** will monitor field equipment and perform cyber-threats detection and (in specific cases) start an automatic reaction. Then, at a higher level, information from the field, after having been properly filtered, aggregated and translated by adaptors (between CI devices and the

CockpitCI system components), will be composed with other global (CI-level) and remote information and elaborated by an **on line risk predictor.** The risk predictor will forecast **QoS of CI delivered services** and perform both situation and impact assessment, evaluating possible cascading effects of cyber threats and thus making possible to implement effective responses to threats. It will make use of adaptive algorithms and exploit proper interdependency models. The output of the risk predictor will be not only provided to the operators, but also back to the field detection and reaction layer, increasing awareness of local components (resulting in increased detection and reaction capabilities). This last feed-back information will also allow devising **smart RTU policies** and dynamic **perimeter intrusion detection strategies**. Finally, near real-time exchange of information between the detection layer and the prediction layer, as well as the exchange of information between interdependent linked CIs (and, possibly authorities or third entities) will be granted in a secure and reliable way by a **secure mediation network**.

System requirements described in the document will reflect the needs and criticalities emerged in the course of the analysis of the proposal [2] and discussion with end-users and consortium partners. The requirements identified in this document will be taken into account for designing the CockpitCI *target reference architecture* (Task 5002). Nevertheless, the CockpitCI *target reference architecture* and the CockpitCI system actually implemented for the final project demonstration will be a particularization to a *specific CockpitCI implementation scenario*. Therefore, the CockpitCI system actually implemented for the project demonstrator is expected to comply with just a subset of the identified requirements (i.e. requirements defined in Task 2002 – Reference Scenario, see deliverable D2.2 as stated in the project proposal [2]).

Then, in this same document, after having introduced the high-level description of the architecture of the CockpitCI system and the functionalities of the main components involved, also the high level requirements of the on-line integrated risk predictor, the detection layer and the secure mediation network will be given, compatibly with what is possible to define at this stage.

Sub-system requirements will be further detailed and refined in subsequent tasks of the CockpitCI project which will address the main components of the CockpitCI system, such as the Cyber Analysis and Detection Layer (task 3001), the On Line Risk Prediction Tool (task 4001), and SCADA Adaptors (task 4002).

1.1 Document Structure

The remainder of the document is organized as follows: Subsections 1.2, 1.3 and 1.4 present, respectively, a glossary of relevant terms, a list of acronyms and symbols that recur in the document, and the definition of an agreed identity code for tracing the identified requirements.

Section 2 gives an overview on SCADA systems, outlying the ongoing process of migration from closed and proprietary solutions to interconnected architectures and “open design” technologies. Also, a typical SCADA reference architecture is presented in Subsection 2.1, where the main components and functionalities are also described. Subsection 2.2 presents a discussion on the SCADA vulnerabilities and possible cyber attacks which may exploit them.

Section 3 introduces the reader to the ambitious CockpitCI vision, which ultimately aims at achieving convergence among business continuity and cyber security, by blending the two worlds of SCADA control systems and cyber-security. Then, objectives of the project are illustrated in Subsection 3.1, while Subsection 3.2 discusses the main assumptions on which the project’s results will be based.

Section 4 presents a discussion of user requirements, as emerged from the analysis of user needs and desiderata. For convenience, user requirements have been listed in a table in Subsection 4.1.

Section 5 deals with system requirements. System requirements have been divided into two main categories: functional system requirements (i.e. the functionalities the system should implement, Subsection 5.1) and not functional system requirements (i.e. how functionalities should be met, Subsection 5.2). Then, functional requirements have been further detailed, distinguishing among requirements related to detection of cyber threats (Subsection 5.1.1), to classification of cyber threats (Subsection 5.1.2), building situation awareness (Subsection 5.1.3), reaction to cyber threats (Subsection 5.1.4) and secure data exchange (Subsection 5.1.5). For the readers' convenience, functional and not functional requirements have been summarized, respectively, in Subsection 5.1.6 and Subsection 5.2.1. Finally, Subsection 5.3 reports a requirements traceability matrix, which traces the relationship between system requirements and user requirements.

Section 6 reports a first and high-level statement of requirements related to three macro components of the CockpitCI tool: the detection layer, the integrated on-line risk predictor and the secure mediation network. A description of these subsystems, along with a general discussion about the CockpitCI architecture is reported at the beginning of the section, so that the reader can easily follow the subsequent discussion of specific subsystem requirements. In particular, on-line integrated risk prediction requirements are discussed in Subsection 6.1, cyber detection layer requirements in Subsection 6.2 and secure mediation network requirements in Subsection 6.3. As usual, requirements are then summarized in tables, reported, respectively, in Subsection 6.1.1 (on-line integrated risk prediction requirements), Subsection 6.2.1 (cyber detection layer requirements) and Subsection 6.3.1 (secure mediation network requirements).

Section 7 contains the conclusions of this work, while Section 8 lists the references cited throughout the document.

Finally, at the end of the document, Appendix A reports the end-user questionnaire that has been submitted to the end-user partners of the project. The answers of IEC, Lyse and TRANS are reported, respectively, in Subsections A.1, A.2 and A.3.

1.2 Glossary

Terminology	Description
Adverse event	Any event which may cause a degradation of the capability of the CI to provide its services.
Critical Infrastructure	A national or transnational asset which is deemed essential for the maintenance of vital societal functions. It could be in the field of health, safety, security, economic or social well-being of people.
Cyber attack	A global intrusion plan that enables the intruder to achieve his malicious objective.
Industrial control system	Industrial control system is a general term that encompasses several types of control systems used in the industrial sector, including supervisory control and data acquisition (SCADA) systems used to control Critical Infrastructures.
Potential cyber attack	Simple and/or composite security event which represent *symptoms* of possible attacks
Risk	A combination of the probability/likelihood for an accident to occur and the resulting negative consequences if the accident occurs.

SCADA operator	Personnel in charge of managing a CI in order to deliver the requested services.
SCADA system	The set of elements which perform supervision and control of an industrial process or a Critical Infrastructure, including the proprietary communication network which links the field devices to the control centre.
Security alarm	Alarm released in presence of a potential cyber attack with variable degree of confidence
Security event	Event that might be potentially relevant, from a cyber security point of view
Security operator/staff	Personnel in charge of the security of the CI.
System of Systems	An interdependent network of Critical Infrastructures
Service	It is what an infrastructure produces and makes available to its customers or other infrastructures.

1.3 Acronym and symbols

Acronym or symbols	Explanation
ARP	Address Resolution Protocol
CERT	Computer Emergency Response Team
CI	Critical Infrastructure
CRUTIAL	Critical Utility InfrastructurAL Resilience
DB	Data Base
DL	Detection Layer
DMZ	Demilitarized Zone
DNP	Distributed Network Protocol
DoS	Denial of Service
DNS	Domain Name System
EMS	Energy Management System
ENTSO-E	European Network of Transmission System Operators for Electricity
EU	European Union
FP	Framework Programme
FR	Functional Requirement
HMI	Human-Machine Interface
HW	Hardware
I/O	Input/Output
ICS	Industrial Control System
ICT	Information and Communication Technology
IDS	Intrusion Detection System

IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IPS	Intrusion Prevention System
IRP	Integrated Risk Prediction
ISO	International Organization for Standardization
LAN	Local Area Network
MICIE	systeMIc risk analysis and secure mediation of data exchanged across linked CI information infrastructurEs
MPLS	Multi Protocol Label Switching
N.A.	Not Applicable
NFR	Not Functional Requirement
PIDS	Perimeter Intrusion Detection System
PLC	Programmable Logic Controller
QoS	Quality of Service
QA	Quality Assessment
RTU	Remote Terminal unit
SCADA	Supervisory Control and Data Acquisition
SDH	Synchronous Digital Hierarchy
SI	System Integration
SLA	Service Level Agreement
SLS	Service Level Specification
SMGW	Secure Mediation Gateway
SMN	Secure Mediation Network
SONET	Synchronous Optical NETworking
SoS	System of Systems
SW	Software
STM	Synchronous Transport Module
TCP	Transmission Control Protocol
TDM	Time Division Multiplexing
UDP	User Datagram Protocol
UR	User Requirement
US-CERT	United States- Computer Emergency Response Team
USB	Universal Serial Bus
VPN	Virtual Private Network
WEP	Wired Equivalence Privacy
Wi-Fi	Wireless-Fidelity
WLAN	Wireless Local Area Network

WP	Work Package

1.4 Identity Code of Requirements

The notation used in this document to provide an Identity Code to all the requirements is the following one:

ElementShortName_ReqNumber, where “ElementShortName” can assume the following values: **UR** (for End-Users driven Requirements), **FR** (for system Functional Requirements), **NFR** (for system Not Functional Requirements), **DL** (for Detection Layer requirements), **IRP** (for online Integrated Risk Prediction requirements), **SMN** (for Secure Mediation Network requirements).

Furthermore, system requirements are classified and prioritized based on their importance and relevance with respect to the development of the CockpitCI tool.

In particular, *shall* is used to refer to requirements that the CockpitCI tool must necessarily meet (“non-negotiable” requirements). *Should* is used to refer to requirements whose implementation is highly recommended, but not mandatory. *Could* is used to refer to “nice to have” requirements, whose implementation is not mandatory, nor highly recommended.

2 Context

For many decades SCADA systems have been isolated systems built on proprietary technology, at the core of critical infrastructures and industrial plants operations. Proprietary SCADA systems are now becoming the exception and even if few cyber attacks against SCADA facilities have been reported until now, today there are many reasons to affirm that the current generation of SCADAs and their controlled CIs present more cyber vulnerabilities [3].

In the past, SCADA operations were performed in isolated environments, all communications among SCADA components were supported by isolated networks and rarely sensible information was shared with the outside world. However, for practicability and efficiency reasons, nowadays SCADA systems are connected to corporate networks and the Internet. Therefore, even control systems designed to be closed to the controlled plant are not perfectly isolated, and can be accessed from the outside. For such reasons nowadays enterprises exploit different levels of firewalls, together with reverse proxy servers and demilitarized zones (DMZ), to grant external authorized users access to enterprise public services [4]. Such commonly adopted solutions lead to a powerful and sophisticated security enforcement; however, as the software complexity increases, security flaws rise up; such flaws become weakness points ready for exploitation [5].

Given the need of connectivity and the decreasing price of hardware and software commodities, many control systems employ solutions such as TCP/IP networking and off-the shell hardware. The exploitation of commercial commodities not only leads SCADA components to inherit the same vulnerabilities, but in the case of “open design” technologies (e.g., TCP/IP, Ethernet, 802.11 WLAN, Web Services etc.), adversaries might dispose of publicly available knowledge (e.g., source code) to deploy their cyber attacks.

From the field equipment point of view, nowadays there are sophisticated controllers made up of microprocessors and embedded operating systems. These controllers may provide many new functionalities, such as flexible configuration via a web server, and digital communication capabilities that allow remote access and control. The increased complexity of the software base may also increase design and implementation flaws, and, hence, increasing the numbers of vulnerabilities open for exploitation. For the mentioned reasons, and the always growing level of complexity of the monitoring and control tasks, SCADA systems and their controlled CIs are more and more exposed to cyber threats of various nature.

The tremendous evolution of sophisticated malwares and cyber attacks carried out in the last few years (e.g. STUXNET, DUQU), exploits the above mentioned weakness points, and makes us think that many actors are currently investing resources in cyber war. Given the high level of intelligence involved, there are reasons to think that these actors could be much more than just hackers, but also national governments aimed to protect economic and political interests of their own and allied countries.

In the next section a generic SCADA reference architecture and the description of its main components are provided.

2.1 Classical SCADA architecture

In this section the SCADA reference architecture is described, by analysing the main components of a SCADA system (see [3] and [6]). For fault-tolerance purposes, SCADAs are usually designed with significant redundancy built into the system, which is not included in the present architecture description. Figure1 shows the mentioned architecture.

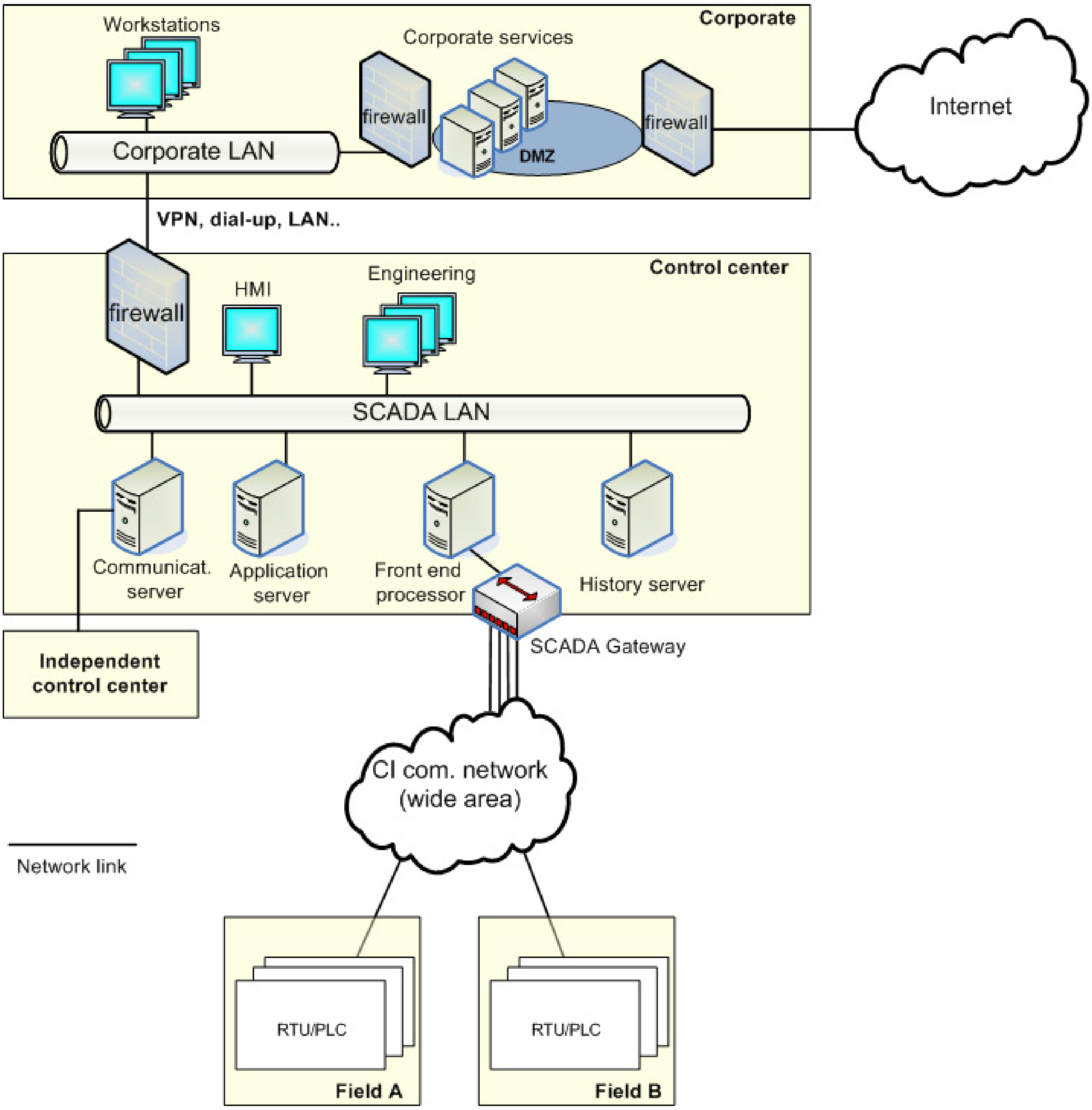


Figure 1: Generic SCADA reference architecture

As can be seen from Figure 1, three main areas can be identified: corporate, control and field area.

Starting from the top, there is the corporate network hosting many workstations used for the most various purposes (remote configurations of SCADA machines, calculate statistics, trends, business activities etc.). The corporate is connected to the Internet for various reasons; in this setting consolidated enterprise security solutions are deployed in more or less sophisticated configurations (DMZ, firewalls and proxy servers). This is made to allow corporate employees to access filtered external services and is also made to publish enterprise services. Workstations in the corporate network can be connected to the SCADA control system through different network connections (VPN, LAN, dial-up modems etc.) and communicate with an application server that handles various services offered inside the control centre. References [7] and [3] underline how such communications channels (even trusted) can be exploited to carry out cyber attacks.

The SCADA control centre performs a centralized monitoring and control of the field processes by means of field interface devices and long distance communication networks. Based on information received from remote stations and devices, automated or operator-driven supervisory commands can be pushed to field devices. All information coming from the field to the SCADA front end are stored in a proper database and handled by the Historian server, to be accessed by business and local workstations (through the application server). The control centre can be distributed over different sites, to this aim an interface toward external systems is supported by a communication server. Inside the control centre we have the HMI (Human Machine Interface) used by an operator to monitor and control the CI, and many engineering workstations deployed to enforce control tasks, analyse data and manage SCADA systems.

Field devices control local operations such as opening and closing valves or breakers, collecting data from sensor systems, and monitoring the local environment for alarm conditions. At this level there are RTUs (Remote Terminal Units) and PLCs (Programmable Logic Controllers). PLCs are programmable controllers aimed to automatize local CI's processes. PLCs are connected to sensors and actuators with a set of I/O channels and are designed to operate in perfect autonomy. They are not aimed at being interfaced with a master system, that means they control sensors and actuators by itself without the help of a supervisor, however they provide an interface to the SCADA control centre for management operations (e.g., read status, switch on/off etc.). RTU is a special purpose data acquisition and control unit, designed to actively interact with a remote control centre. Its main purpose is to collect sensing data from a monitored process, and send them to the control system. The control centre is able to influence CI's physical processes by sending instructions to RTUs; such instructions are further executed by RTUs by properly interacting with their connected actuators (valves, mechanical systems, electrical switches etc.). Data generated at field level are transmitted over the long distance CI's communication network, to reach the control centre.

The CI's communication network can cover great distances, and is built upon a high number of network protocols, devices and communication media. The communication network structure follows a hierarchical design, and is composed by end-devices connected to an access communication network, and communicating across long distances through a high capacity transport communication network [8] [9]. CI communications can have stringent constraints in terms of QoS, security and reliable delivery; for such reasons two approaches are possible a) the network is owned by the CI operator and is reserved for SCADA transmission only, b) SCADA communications are transmitted across the network of a telecommunication operator; in this scenario specific Service Level Agreements (SLA) can be stipulated in order to accommodate CI communication requirements. Even if both approaches are possible, the possibility to exploit the telecommunication network could be more attractive, given its lower price and given the evolution of Future Internet network services. The FINSENY [18] project hopes to connect the SCADA traffic of next generation smart grids to Future Internet networks, since they could fit exactly their tight transmission requirements at much lower cost. The following picture describes the general communication network architecture of a CI. Note that many different architectural and technological solutions are possible for SCADA communication networks; therefore the purpose of the following paragraphs is not to describe the solution adopted in every system, but to give a reference scheme to be taken into account while addressing SCADA communications.

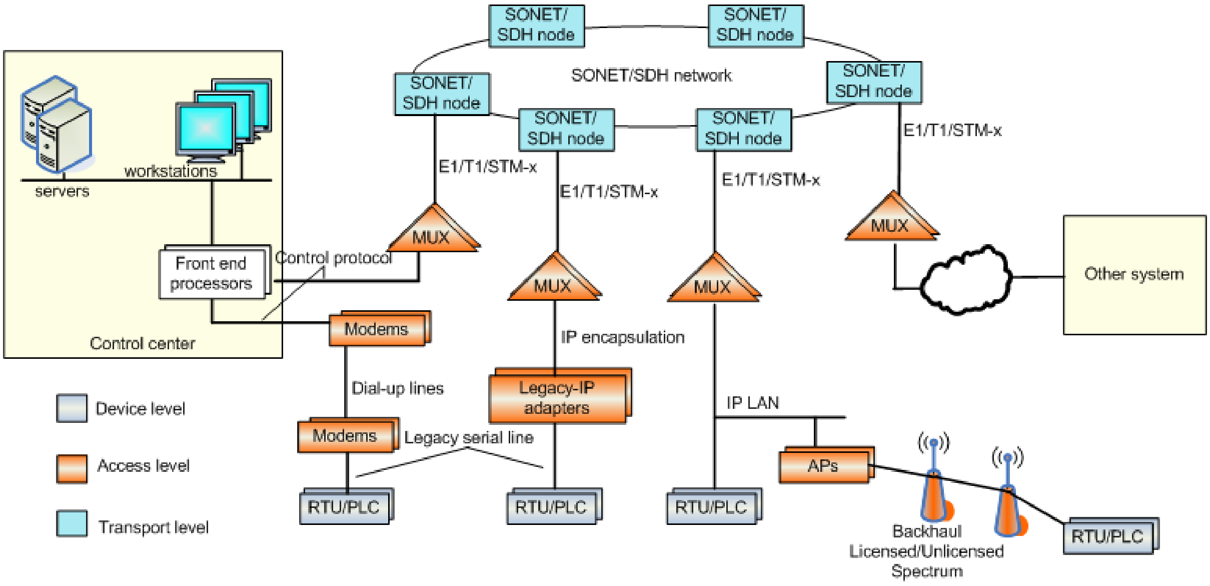


Figure 2: General architecture for the CI's communication network

Usually, legacy CI communication networks deploy TDM multiplexers to achieve communications between their systems. A dedicated circuit or channel is created and reserved for a single communication instance and available to the user at all times. The assigned bandwidth remains constant and traffic is transmitted at wire-speed with minimal delay.

Despite the big diffusion of TDM circuit based SCADA communication networks, today IP based technologies represent the actual choice for different reasons (management complexity, money, bandwidth efficiency etc.); therefore the trend is to perform a smooth migration from the old deployed TDM networks (circuit-switched) to the current generation of IP based infrastructures (packet-switched). Such migration can be supported by different practical solutions [5] aimed to make legacy TDM and not legacy IP technologies running together over the same infrastructure, avoiding the effort of deploying and managing two different parallel networks.

The size of network trunks connecting field devices to the control centre, as well as the kind of access technology employed to perform the access (dial-up modems, LAN, radio backhaul, Wi-Fi etc.), may vary significantly [6]. Field devices are controlled and/or managed by the control centre through a control protocol running over TCP/IP or other different transport, network and framing technologies, even legacy.

For the long distance there is E1/T1/STM-x multiplexers injecting CI communication traffic into the TDM based SONET/SDH core. It is possible to note that a packet based backbone (MPLS, Gbit Ethernet etc.) instead of the legacy SONET/SDH might be found [5].

2.2 Vulnerabilities and possible attacks

This section explains main SCADA vulnerabilities and possible attacks based over them. On the basis of the studies carried out in [10], SCADA vulnerabilities can be classified into three different classes:

Architectural vulnerabilities: directly derive from the adopted architecture of the SCADA system. Different types of vulnerabilities can be identified at this layer:

- *Field network easily reachable from the control centre*: Usually an attacker is considered unlikely to reach this area, which represents the inner part of the system. Thus security levels at the bridge with this area might be lower.
- *Trust and Security infrastructures*: traditionally communications among components of the SCADA were performed in closed and secure environments. However with the smooth migration to open networking standards, the deployment of effective security infrastructures is strongly required, but in many cases not fully addressed.
- *Single points of failures:* in many cases some SCADA components represent single points of failures, and are badly supported by proper redundancies (redundant network trunks, server replications, smart firewall and proxy topologies etc.).
- *Radio technologies:* the wide exploitation of radio technologies, spread all over field sites, control centres and corporate buildings, makes infrastructure owners saving much money, at the expense of cyber security drawbacks.

Security policies: even the SCADA system with the most robust architecture, becomes unsecure if security policies are badly, or not fully applied. A list of possible faults in the application of security policies is presented:

- *Unpatched systems:* since SCADA servers and workstations don't run patched versions of software, they are extremely vulnerable. The reason of using unpatched tools, is because on SCADA systems is not rare to find ad-hoc made software, then whenever a released patch is applied, new integration tests must be performed in order to verify compliancy with the base system; such integration task could be a complex activity and might generate inacceptable system down times [4] [10].
- *Few antivirus updates:* often inefficient antivirus update policies are applied; that is to avoid to connect machines to the Internet (for antivirus updates) or to avoid the introduction of new servers and infrastructures aimed to dispatch updated antivirus signatures. Both operations are cumbersome, then antivirus signatures are updated rarely, and the control system's network is kept as much isolated as possible.
- *"One-time" security assessment:* SCADA infrastructure evolves over the time with the introduction of new devices and technologies. Sometimes such evolution is not fully documented, and iterative security level estimations are never performed, or are not in line with the SCADA architecture enhancement.
- *Bad management of user credentials:* Often, even in large enterprises, passwords or login data are not handled and maintained with care. This may lead malicious individuals to steal and exploit such sensible information.

Software and protocols:

- *Software bugs:* software bugs may arise at any time during its utilization, and may be exploited to harm the system in several ways. Software bugs may exist for different reasons: coding errors, patches incompatibilities, wrong input handling, unhandled exceptions and so on.
- *SCADA protocols*: most SCADA protocols, such as Modbus and DNP were designed years ago to monitor and control field devices over serial connections, in closed and secure environments, without any means for authentication and security purposes. However with the wide spread of open standards as base technologies for SCADA operations, many SCADA protocols were encapsulated over TCP/IP connections, without improving their lack of authentication and encryption capabilities, proper of their native applications.

A subset of possible attacks that might be performed against a SCADA system is listed below:

1. *Issue unauthorized commands to field control equipment*
   The lack of trust and security mechanisms of many SCADA protocols, as well as the wrong or inexistent fulfilment of security policies, can lead an adversarial to impersonate the SCADA master and issue unauthorized control commands to field devices. Since slave devices can neither verify the identity of the master, nor packet integrity, an attacker can easily forge hand-made legal packets (for example sending false time synchronization to field SCADA devices) or replay past transmitted packets. Another possibility involves the exploitation by an intruder of stolen administration credentials (through email fishing, DNS spoofing, VPN security flaws etc.) to logon into the system and issue unauthorized control instructions.

2. *Delay or block the flow of information through the control network*
   Communication flows between SCADA master and slave devices are critical, and subject to tight constraints in terms of delay and reliable delivery. An attacker may use different approaches to generate interferences across such communication channels. Man-in-the-middle [1]techniques allow an attacker to intermediate between the SCADA master and the front end gateway, to intercept the whole control traffic and interfere with the delivery of messages. Another possibility for an attacker to interfere with the control traffic delivery is to generate a huge amount of control packets toward the master's network card, delaying the delivery of not malicious packets. In order to accelerate the effects, it could use for example a UDP packet generator (it is easier to generate a huge amount of traffic using UDP instead of TCP).

3. *Send false information (statuses and/or alarms) from field control equipment toward a central SCADA.*
   As a consequence of the vulnerabilities of SCADA protocols, an attacker that has granted access to the control centre LAN can find easy to impersonate a set of slaves and provide false information to the SCADA master. Such operation could lead CI operators to take completely wrong decisions, with potentially catastrophic effects. This result can be achieved making slaves unavailable (i.e., through DoS or viruses) before sending fake status messages to the master.

4. *Make unauthorized changes to control system software to modify alarm thresholds or other configuration settings.*
   The bad fulfilment of security policies and the presence of software bugs can be exploited to perform malicious system reconfigurations. There are different ways for an attacker to gain root permissions on the system and make reconfigurations, which range from stealing credentials with fishing or spoofing, to the gaining of root permissions through dialup connections. Malware diffusions are also dangerous, since viruses can infect SCADA machines and disrupt system settings. Such infection diffusions can also begin at the business network and propagate by means of existing connections to the control centre.

5. *Make resources unavailable or influence their behaviour by propagating malicious software (e.g. a virus, worm, Trojan horse) through the control network.*
   Once again software bugs and SCADA protocol flaws play a key role in the achievement of such result. Resources can be made unavailable in different ways; for instance errors in the implementation of SCADA protocols can be exploited to make field and master devices stop running, or reset. These vulnerabilities can be exploited to obtain buffer overflows,

[1] Man-in-the-middle can be easily achieved in LAN and WLAN networks by means of ARP spoofing techniques.

device de-synchronization, bugs in the handling of exceptions and so on. Other possibilities are to send ad-hoc messages or replayed messages to reset or stop devices, or to instruct them to work without the master supervision. Also DoS attacks toward master or slaves can make them unavailable as well as virus infection that may heavily influence the behaviour of field RTUs and PLCs.

6. *Unauthorized interception of control commands and information (physical, algorithms, software, etc.).*
   With SCADA machines and devices running TCP/IP stacks enable attackers to connect the same networks and sniff the traffic transmitted across. This practice can lead to collect sensible information (i.e. administrative credentials) and infer the logic of algorithms running at connected machines. Moreover network sniffing is the ground procedure for Layer-2 password cracking (i.e. WEP cracking) and man-in-the-middle attacks that exploit well known TCP/IP suite flaws (i.e. for ARP spoofing).

3 CockpitCI vision

The vision of CockpitCI is in line with the MICIE project [11] of which it resumes the main concept, i.e. that by increasing the cooperation among infrastructures it is possible to provide the operator with a better situation awareness in the presence of adverse events and therefore increase the CI level of service (business continuity). CockpitCI proposes this concept again in a wider operational range which addresses now not only adverse events but also cyber events.

The world of Industrial Control System 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 a superior level of awareness (global awareness). The CockpitCI vision is that the convergence among business continuity and cyber security is possible with positive fallouts for all the involved players. From the point of view of security staff benefits will arise thanks to the availability of new security data coming from the process network. Such data will be collected by local SCADA-oriented detection agents able to recognize traffic anomalies or intrusions attempts. Then, they will be merged, to build a wider cyber awareness, with the traditional ICT networks security related data. From the business point of view, a near real-time risk evaluation capability, exploiting also the previously built cyber awareness, will allow a clever reaction by SCADA operators to possible cyber threats and the avoidance of large domino effects. Starting from the improved risk definition, it will be also possible, for the stakeholder, to have a better tailored definition of service level agreement (and then contracts) with its customers. It is not just a question of putting together the two worlds of SCADA industrial control systems and cyber-security, but of reshaping the boundaries of each and blending the two by taking advantage of each other strengths.

Such global awareness will be fostered by fusing the information which originates from the various control rooms of the infrastructure, from the control rooms of interdependent CIs, from the control rooms at national level which are again connected with the intelligence at national and transnational level. The cyber issue is not a local problem which may be confined in a restricted boundary, but it is rather a transnational problem which goes beyond national boundaries. Therefore, the various functions of the CockpitCI tool must not be isolated.

CockpitCI will make a further step ahead by putting together the local perspective provided by information collected from the field equipment with the global perspective at CI level: the local perspective refers to the smart elements at the field level which will monitor equipment and devices and perform cyber threat detection and eventually start an automatic reaction; the global perspective refers to the wider perspective on the state of the System of Systems which, thanks to increased cooperation among infrastructures and shared interdependency models, is wider compared to previsions that can be generated by sector specific and isolated simulators. Putting the two levels to work together will be the basis for a smarter reaction capability, aiming at a graceful degradation, aiming at understanding how much of the system can be kept in operation safely in adverse situations and maintaining at least partial operations rather than total shutdown.

Having in mind the vision of the project described above, project objectives and main assumption about the behaviour of the CockpitCI system have been obtained and described in the following sub-sections.

3.1 Objectives

The main objectives of the CockpitCI project as extracted from the project proposal [2], further refined through discussions among Consortium's partners are listed below.

Objective #1:
CockpitCI aims at improving the resilience and dependability of Critical Infrastructures (CIs) by the automatic detection of cyber threats and the sharing of near real-time information about attacks among CI owners. This objective highlights the importance of achieving cyber awareness and to achieve it beyond the boundary of the single CI. The importance of sharing near real-time information among CI restates the main concept of the MICIE project [11] and it is stemming from the interdependency among CIs. This is in line with [16] which states: "Security improves through greater Situation Awareness: gaining the ability to understand what is happening beyond our network boundaries to detect threats on the horizon".

Objective #2:
CockpitCI aims at identifying, in near real-time, the CI functionalities impacted by cyber-attacks and at assessing the relevant degradation of CI delivered services. This information should be conveyed to SCADA and security operators to greatly increase their awareness of the situation and improve their capability to handle the situation.

Objective #3:
CockpitCI aims at classifying the associated risk level, broadcasting alerts at different security levels and activating strategies of containment of the possible consequences of cyber-attacks.

Objective #4:
CockpitCI aims at leveraging the ability of field equipment, in coordination with the central control level, to counteract cyber-attacks by deploying preservation and shielding strategies able to guarantee the required safety.

Objectives 3 and 4 address the need to add intelligence and implement reaction at the global and local level.

3.2 Main assumptions

In this section general, assumptions about the global CockpitCI system and about the role of system components will be addressed. All these assumptions are in line with the CockpitCI objectives listed in the previous section and are all considered very reasonable in the light of the consortium partners' experiences and discussions with the end-users. Hence, these assumptions, will be treated as true for the rest of the project.

1. Adverse events with special focus on cyber attacks will be considered. Physical security is considered limited to physical CI (Critical Infrastructure) vulnerabilities that can lead to cyber attacks.
2. Brute force physical sabotage such as cutting wires and cables or hammering devices and radio jamming are out of the scope.
3. The CockpitCI tool is associated with a specific CI and will be able to interoperate with other CockpitCI tools located in other CIs, as identified in the Reference Scenario.
4. In the reference scenario at least two CI will be considered in order to evaluate the propagation of cyber attacks through CI interdependencies.
5. The following general cyber attack scenarios, which describe undesired behaviours in the SCADA system, have been identified as of interest for the project:
    a. issuing unauthorized commands to field control equipment (for example sending false time synchronization to field SCADA devices), which may cause for example the opening or closing of circuit breakers in the power network;
    b. disrupting control system operation by delaying or blocking the flow of information through the CI communication network;

c. sending false information (statuses and/or alarms) from field control equipment toward a central SCADA, which could cause the CI operator to have a false picture of the underlying process and therefore initiate inappropriate actions;
d. simulating a vulnerability to the level of CI services that may induce the operator of dependent CI to make the wrong decisions;
e. sending false time synchronization to field SCADA devices;
f. making unauthorized changes to control system software to modify alarm thresholds or other configuration settings;
g. rendering resources unavailable or with a relevant degradation of behaviour by propagating malicious software (e.g. a virus, worm, Trojan horse) through the control network;
h. unauthorized interception of control commands and information that may lead to the knowledge of vulnerabilities of the critical infrastructure (physical, algorithms, software, etc.) for support of future attacks.

6. The CockpitCI tool shall be validated against a subset of cyber attacks identified in the Reference Scenario (the Reference Scenario will be developed in Task 2002).
7. CockpitCI functionalities *shall* address a selection of the following aspects defined in the Reference Scenario:
   - SCADA and enterprise network vulnerabilities;
   - Cyber threats to SCADA and enterprise network;
   - Different sources of attacks and different attacker profiles;
   - The pre-existent security policies and security solutions of SCADA and enterprise network;
   - Attack scenarios;
   - Realistic consequences of successful attacks on SCADA services (i.e. Fault Isolation and System Restoration) and in turn on CI services (i.e. power to grid customers);
   - A worst case attack scenario (i.e., with severity of consequences on CI services (i.e. large power grid black outs at regional/national level).

4 End-User perspective: needs and requirements

This section addresses the end-user perspective and reports the list of end-user requirements for the CockpitCI system, which have emerged from analysis of the proposal document [2] and discussions with the end-users. To ease the discussion with end-users, a questionnaire was also prepared to address specific issues; questionnaires, as filled by end-users, are reported in the Appendix.

Situation Awareness was stated in the previous section as one of the main objectives of the project and the end-user questionnaires have confirmed the importance of assuring that the CockpitCI tool *shall* improve, in terms of quality and timeliness of the information, the situational awareness and support the decision making capability of the SCADA operator in presence of adverse events, with particular regard to cyber-attacks (**UR_1**). As a matter of fact the awareness over the System of Systems integrated with cyber awareness could greatly increase the ability of the operator to handle the situation.

Moreover, it is also important that the CockpitCI tool *shall* improve the situational awareness and support the decision making of the cyber-security staff in presence of cyber-attacks (**UR_2**). The two requirements, UR_1 and UR_2, have been stated separately in order to highlight the fact that the SCADA and security operators have different needs and knowledge and their areas of decision making are also distinct.

Speaking in a holistic fashion, it is evident that from the end-user perspective the CockpitCI tool *shall* improve business continuity and resilience of services delivered to Critical Infrastructure customers in presence of cyber-attacks (**UR_3**).

In order to fulfil these objectives the CockpitCI project approach is to early detect cyber-attacks and, in case of attack-in-progress, to adequately react and contrast the attack. In this context the CockpitCI tool *shall* detect in near real-time cyber-attacks (including 0-days attacks, i.e. attacks to system vulnerabilities that have never been identified in the past) against the SCADA system (**UR_4a**). This requirement is clearly understandable from the end-user point of view, especially in the envisaged scope of CockpitCI, yet it is too generic. There is clearly the need to restrict in some way the domain of possible cyber attacks in a reasonable way; this may be done preliminarily by referring to the cyber attack scenarios listed in paragraph 3.2. There are also a number of attacks that are only detectable using medium-term correlation windows. The cyber detection layer of CockpitCI will support “near real-time” detection for a large number of cyber attacks, but not for all types of cyber attacks, since this is not feasible with current technology.

The automatic reaction capability of the CockpitCI tool is also a controversial issue, and, as stated in the proposal [2], “*until now such solutions have been completely rejected by CI operators because they fear that local automatic reactions may happen during “normal” activities inducing catastrophic behaviour*”. Yet a reaction capability may be important in order to quickly and effectively react to adverse events that may occur over the System of Systems and, in particular, to face cyber attacks.

Following from the questionnaire posed to end-users (see Appendix), it seems acceptable that in pre-planned situations the CockpitCI tool may automatically start a reaction and also that in some extraordinary situations the field equipment may enter an "attack mode", ignore further commands and stay in a predefined state for a period of time. Starting from this point, it is possible to go ahead with the automatic reaction capability approach, even though this must be carefully planned and analyzed, and include a requirement such as: “The CockpitCI tool shall isolate and react to cyber-attacks against the SCADA system” (**UR_4b**).

At the same time the end-user requires that the detection, isolation and reaction strategies of the tool *should* minimize the perturbations on QoS to customers in terms of business continuity and resilience of services to CI customers (**UR_5**).

In case of attack-in-progress, some portion of the whole system could have been compromised; in this context the CockpitCI tool *shall* identify the compromised sections of SCADA, ICT and in turn of the domain CI (**UR_6**).

The CockpitCI tool *shall* inform in real-time the security staff about the security state of the CI, the location and severity of the attack, action performed and the result of the correction action performed (**UR_7**).

The concept of the CockpitCI tool is that it has to support the operation of the SCADA system. In this context, it is important that the CockpitCI tool *should* not alter or interfere with the normal operations of the SCADA system (**UR_9**), where the term “normal operations” refers to situations without cyber attacks. Of course, since it is always necessary to balance the risk of system compromise by an intruder with the risk of potentially degrading system operability, the above statement should be further analysed to understand how it can be realistically carried out. As a matter of fact it may clash for example with the idea of providing some kind of automatic reaction capability. It will be further addressed in the System requirements section.

From the end-user perspective, it is also desirable that the CockpitCI tool *shall* not overload the SCADA operator with an excessive rate of false alarms (**UR_10**); this is a critical requirement and it is not realistic at this stage to claim an extremely low false alarm rate, since there is a limited literature and very little practical experimentation on this issue. In addition the detection of “zero-day attacks”, by nature, will result in a non predictable number of false positives. In order to provide a flexible and adaptive solution, the CockpitCI tool *may* support mechanisms to progressively adjust its sensitivity and progressively reduce the rate of false positives/false negatives.

The expectation is also that the CockpitCI tool *shall* be a scalable solution (i.e. it *shall* be feasible for CIs of any type, number and dimensions) (**UR_11**). Of course some kind of customization will be needed.

The CockpitCI tool *should* cost reasonably (**UR_12**). The reasonability of the cost of course is related to the possible loss or damage in service level.

The current situation of the SCADA domain imposes that novel solutions have to integrate with already existing structures and equipment deployed in Critical Infrastructures; in this context, it is important that the CockpitCI tool *shall* be effective both on new SCADA HW/SW, as well as legacy SCADA HW/SW (**UR_13**), and that the CockpitCI tool *shall* be compatible and possibly integrable with other cyber security defence software and will contribute to form a multi-layer cyber defence (**UR_14**).

It is also required by the end-user that the CockpitCI tool *should* not use the SCADA communication infrastructure, but *should* provide its own communications means (**UR_15**). Nevertheless, it seems reasonable to take into consideration the case in which the CockpitCI tool may also use the existing communication infrastructure (due to cost or technological constraints), albeit with possible sacrifice of functionalities/performance.

The CockpitCI tool *shall* interface with the operators (through the HMI) in an efficient way, in order to communicate at best its outcome. It *shall* provide an “intuitive” user interface that will provide the SCADA and security operators only with necessary information for decision making in uncertain situations (**UR_16**). In these situations the operator is already receiving a lot of information from the field and has not enough time to analyse more information. This requirement also reflects the choice of the acronym of the project which refers to providing an effective and instrumental interface to the CI operator.

In coherence with CockpitCI vision, the CockpitCI tool *should* also improve synergies between SCADA control and cyber security (**UR17**). This requirement needs to be further clarified, yet it addresses the need to have an efficient exchange of information between the SCADA and security operators.

And finally, and here we move back to the discussion about automatic reaction, the CockpitCI tool shall be configurable to a passive mode where attacks and suspicious traffic is detected and reported, but no active actions are taken (**UR18**).

4.1 End-Users requirements summary

The following table summarizes the defined end-user requirements identified in the previous section.

Requirement id	Short description
UR_1.	The CockpitCI tool *shall* improve the situational awareness and support the decision making capability of the SCADA operator in presence of cyber-attacks
UR_2	The CockpitCI tool *shall* improve the situational awareness and support the decision making of the cyber-security staff in presence of cyber-attacks
UR_3	The CockpitCI tool *shall* improve business continuity and resilience of services delivered to Critical Infrastructure customers in presence of cyber-attacks
UR_4a	The Cockpit CI tool *shall* detect in near real-time cyber-attacks (including 0-days attacks) against the SCADA system
UR_4b	The Cockpit CI tool *shall* isolate and react to cyber-attacks against the SCADA system
UR_5	The detection, isolation and reaction strategies of the tool *should* minimize the perturbations on QoS to customers in terms of business continuity and resilience of services to CI customers
UR_6	The CockpitCI tool *shall* identify the compromised sections of SCADA, ICT and in turn of the domain CI
UR_7	The CockpitCI tool *shall* inform in real-time the security staff about the security state of the CI, the location and severity of the attack, action performed and the result of the correction action performed
UR_8	Cancelled.
UR_9	The CockpitCI tool *should* not alter or interfere with the normal operations of the SCADA system
UR_10	The CockpitCI tool *shall* not overload the SCADA operator with an excessive rate of false alarms
UR_11	The CockpitCI tool *shall* be a scalable solution
UR_12	The CockpitCI tool *should* cost reasonably
UR_13	the CockpitCI tool *shall* be effective both on new SCADA HW/SW as well as legacy SCADA HW/SW
UR_14	The CockpitCI tool *shall* be compatible and possibly integrable with other cyber security

	defence software
UR_15	The CockpitCI tool *should* not use the SCADA communication infrastructure, but *should* provide its own communications means
UR_16	The CockpitCI tool *shall* provide an “intuitive” user interface that will provide the SCADA and security operators only with necessary information for decision making in uncertain situations
UR_17	The CockpitCI tool *should* also improve synergies between SCADA control and cyber security
UR_18	The CockpitCI tool shall be configurable to a passive mode where attacks and suspicious traffic is detected and reported, but no active actions are taken.

Table 1: End-user requirements

5 System requirements

In this section system requirements will be defined and analysed. This section is divided into several sub-sections: system requirements are divided in functional requirements (*what* the tool will do) and not functional requirements (*how* the tool will perform its functionalities: i.e. timeliness, reliability, graceful degradation and security, in terms of performance, quantity numbers, data integrity, confidentiality and availability); system requirements have also been grouped according to the functionality provided.

5.1 Functional requirements

Functional requirements are intended to be requirements describing what the CockpitCI tool is expected to do. Consistently with the project proposal [2], the main functionalities of the CockpitCI tool have been organized as follows:

- Cyber Attack Detection, in order to detect cyber threats;
- Cyber Attack Identification, in order to identify the type of cyber threats;
- Building Situation Awareness
  - Understand the current situation;
  - Predict the near term evolution of the situation;
  - Risk prediction;
- Reaction:
  - Support the selection of appropriate countermeasures;
  - Provide automatic reaction logics;
- Data Exchange, with neighbouring and interdependent CIs;

In the following the requirements associated to each main functionality are identified.

5.1.1 Cyber Attack Detection

The main objective of the cyber detection layer is that it shall detect cyber-attacks belonging to the types listed in paragraph 3.2 (**FR_1**).The cyber detection layer should also support “near real-time” detection of cyber attacks in order to be able to start a reaction promptly, yet near real-time detection is not feasible for all types of attacks with current technology (there are in fact a number of attacks, such as stealth multistage attacks, that are only detectable using medium-term correlation windows). For this reason the cyber detection layer shall provide near real-time monitoring of the area of interest, i.e. collection, filtering and processing of data, in order to be able to quickly detect potential cyber attacks (**FR_2**). This will allow to detect in near real-time attacks with known signatures and to detect attacks via anomaly detection mechanisms (e.g. unknown attacks) and/or stealth multistage attacks as soon as the malicious source of the pattern/behaviour becomes observable with a sufficient degree of confidence.

With respect to the detection of cyber-attacks, the Detection Layer *should* generate a limited number of false alarms (**FR_3**) in order not to overload the SCADA operator with an excessive rate of false alarms. In order to achieve this result the Detection layer *shall* support mechanisms to be able to gradually adjust the thresholds for false positives and false negatives according to the preference and historical behaviour of the CI operators (**FR_4**).

Cyber attacks may originate within the SCADA system, e.g. by insertion of a compromised USB device, or may propagate through the ICT network to the SCADA system, e.g. from the Corporate network. It is important that both types of attacks *shall* be managed by the Detection layer (**FR_5**).

In order to accomplish the detection of the above mentioned attacks, the CockpitCI tool *shall:*

- Monitor the traffic flows at the boundaries/perimeter of the SCADA system (both inbound and outbound) (**FR_6**);
- Monitor the internal SCADA traffic (**FR_7**).

The CockpitCI tool should be able to detect potential cyber-attacks before they reach and affect the SCADA system (**FR_8**), therefore it is important to extend the detection capability (area of interest) beyond the perimeter of the SCADA system. This may achieved mainly by integrating alarms from other interconnected CIs (**FR_9**) and from other cyber security equipment (not part of CockpitCI) which may be deployed in the network (**FR_10**). Requirement FR_10 implies the need to comply with existing standards, if any, in order to be able to interface properly with other existing security equipment.

Requirement FR_8 is very stringent and may not be achievable in many cases, such as when zero-day attacks occur, it is therefore important that the CockpitCI tool *shall* detect as early as possible cyber-attacks which cause deviations of the major functionalities/services of the SCADA system (**FR_11**).

Industrial Control Networks are different from standard IT networks. In particular, they present more regular traffic patterns, static topologies and available a-priori knowledge (e.g. roles and policies). In this context, it is very important that rather than just reusing IT technologies which were not designed for SCADA and which have not worked very well in the SCADA domain, the cyber detection layer *shall* take into account and exploit the specific nature of industrial control networks while performing cyber attacks detection. (**FR_12**).

The CockpitCI tool *shall* identify the compromised sections of SCADA, ICT and in turn of the domain CI (**FR_13**).

5.1.2 Classification of Cyber Attacks

The classification of cyber attacks is extremely important so that it is possible to set in a precise way the action the system has to execute to handle a certain alert. The alert could trigger automatic countermeasures. Consequences of a misclassification may be significant, just consider the case of a buffer overflow attack where countermeasures should take place immediately (because of possible consequences) and a path traversal attack for which the activation of countermeasures can be delayed. It is therefore fundamental that the CockpitCI tool *shall* identify the type of cyber-attack (**FR_14**). Of course this may be easy when it comes to attacks detected by signature-based mechanisms, whilst it may be extremely difficult or impossible for other types of attacks such as “zero-day” attacks, where anomalies or deviation of behaviour can be detected but not the specific nature of the ongoing attack.

5.1.3 Building Situation Awareness

By situation awareness it is intended the understanding of the current situation and the prediction of what is likely going to happen in the near future. This predictive capability will then guide the system reaction.

There is therefore the need to develop and to employ near real-time models which are able to predict the QoS delivered by SCADA systems and interconnected Telecommunication networks under cyber attacks (**FR_15**).

Thanks to the models developed in FR_15 and to the information exchanged with other CIs, the CockpitCI tool *shall* provide, in near real-time, a CI risk level estimating the degree of belief that in the near future the CI will no more be able to provide the CI services with the desired QoS in consequence of certain undesired events, including cyber attacks, occurring in the reference CI or in other interdependent CIs (**FR_16**).

As a consequence, one of the main objectives of the CockpitCI tool is to send alerts about possible cyber attacks. In this context the CockpitCI tool *shall* be able to provide a level of alert to the SCADA control centre and/or to the cyber security staff (**FR_17**) and also directly to field equipment (**FR_18**), even though it is a matter to be further investigated with end-users if and how this alert may be used by field equipment. The alert may originate at central level or locally.

The CockpitCI tool *shall* provide an “intuitive” interface to SCADA operators (**FR_19**) and another “intuitive” interface to security staff (**FR_20**) to convey the above mentioned relevant information.

In order to improve synergies between SCADA control and cyber security, the CockpitCI tool shall provide an efficient exchange of information between the SCADA and security operators (**FR_21**).

5.1.4 Reaction

In order to react appropriately to an alert situation, the CockpitCI tool *shall* be able to distinguish between a failure due to adverse events and a cyber attack (**FR_22**).

The CockpitCI tool *shall* suggest reaction strategies in presence of cyber-attacks on the SCADA system and on the interconnected ICT network to the SCADA operator and cyber security staff (**FR_23**).

Among the possible reaction strategies, a significant one, which responds to the well-known security principle of “compartmentalization”, is represented by isolating the portion of the network affected by the cyber attack. In this way it may be possible to stop the attack before it propagates to other nodes of the system or it penetrates into the SCADA system. Therefore the following requirement is included: the CockpitCI tool *shall* provide an isolation capability in presence of cyber-attacks on the SCADA system and on the interconnected ICT network (**FR_24**).

It is of course essential that the SCADA operator and the cyber security staff should normally have the final decision on the reaction strategy to contrast an in progress cyber-attack; however, there are situations such as those in which there are timing constraints and/or there is no communication available between the SCADA control centre and the field equipment, where an automatic reaction may be required. The following requirement is therefore included: the level of alert elaborated from the CockpitCI tool, at the global or local level, *could* be used, in specific situations, to trigger automatic and predetermined reactions at the RTUs (**FR_25**). Of course, it is left to the operator to set the conditions which will activate or not such an automatic reaction.

The CockpitCI tool shall be configurable to a passive mode where attacks and suspicious traffic is detected and reported, but no active actions are taken (**FR_26**).

5.1.5 Data exchange

The CockpitCI tool *shall* provide a mean for the single CI to securely and efficiently communicate/receive status information, alerts and security related messages to/from the interconnected and interdependent CIs hosting a CockpitCI tool (**FR_27**).

5.1.6 Functional requirements summary

The following table summarizes the identified and defined functional system requirements.

Requirement id	Short description
FR_1.	The cyber detection layer *shall* detect cyber-attacks.
FR_2	The cyber detection layer shall provide near real-time monitoring of the area of interest in order to be able to quickly detect potential cyber attacks.
FR_3	The Detection Layer *should* generate a limited number of false alarms.
FR_4	the Detection layer *shall* support mechanisms to be able to gradually adjust the thresholds for false positives and false negatives according to the preference and historical behaviour of the CI operators
FR_5	The cyber detection layer *shall* manage both Cyber attacks that may originate within SCADA, and cyber attacks that may propagate from the ICT network to the SCADA system
FR_6	The CockpitCI tool *shall* monitor the traffic flows at the boundaries/perimeter of the SCADA control system (both inbound and outbound)
FR_7	The CockpitCI tool shall monitor the internal SCADA traffic
FR_8	The CockpitCI tool *should* detect cyber attacks before they affect the SCADA system
FR_9	The CockpitCI tool *shall* integrate alarms from other interconnected CIs
FR_10	The CockpitCI tool *shall* integrate alarms from other cyber security equipment (not part of CockpitCI) which may be deployed in the network
FR_11	The CockpitCI tool *shall* detect cyber-attacks which cause deviations of the major functionalities of the SCADA system
FR_12	The Detection Layer shall take into account and exploit the specific nature of industrial control networks while performing cyber attacks detection
FR_13	The CockpitCI tool shall identify the compromised sections of SCADA, ICT and in turn of the domain CI
FR_14	The CockpitCI tool *shall* identify the type of cyber-attack
FR_15	The CockpitCI tool *shall* employ in near real-time models which are able to predict the QoS delivered by SCADA systems and interconnected Telecommunication networks under cyber attacks
FR_16	The CockpitCI tool *shall* provide, in real-time, a CI risk level estimating the degree of belief that in the near future the CI will no more be able to provide the CI services with the desired QoS in consequence of certain undesired events, including cyber attacks, occurring in the reference CI or in other interdependent CIs
FR_17	The CockpitCI tool *shall* be able to provide a level of alert to the SCADA control center and/or to the cyber security staff.
FR_18	The CockpitCI tool *shall* be able to provide a level of alert directly to field equipment
FR_19	The CockpitCI tool *shall* provide an “intuitive” interface to SCADA operators
FR_20	The CockpitCI tool *shall* provide an “intuitive” interface to security staff
FR_21	The CockpitCI tool shall provide an efficient exchange of information between the SCADA and security operators.
FR_22	The CockpitCI tool *shall* be able to distinguish between a failure due to adverse events

	and a cyber attack
FR_23	The CockpitCI tool *shall* suggest reaction strategies in presence of cyber-attacks on the SCADA system and on the interconnected ICT network to the operator
FR_24	The CockpitCI tool *shall* provide an isolation capability in presence of cyber-attacks on the SCADA system and on the interconnected ICT network
FR_25	The level of alert elaborated from the CockpitCI tool *could* be used, in specific situations, to trigger automatic and predetermined reactions at the RTUs
FR_26	The CockpitCI tool shall be configurable to a passive mode where attacks and suspicious traffic is detected and reported, but no active actions are taken.
FR_27	The CockpitCI tool *shall* provide a mean for the single CI to securely and efficiently communicate/receive status information, alerts and security related messages to/from the interconnected and interdependent CIs hosting a CockpitCI tool

Table 2: Functional system requirements

5.2 Not functional requirements

Not functional requirements are intended to be requirements describing *how* the CockpitCI tool will perform its functionalities (described in the previous section): i.e. timeliness, reliability, graceful degradation and security (e.g. data integrity, confidentiality and availability). Many not functional requirements derive from the discussions carried out in the previous sections.

In particular (as stated in [12]), non-functional requirements (also called quality requirements) are requirements that specify criteria that can be used to judge the operation of a system, in contrast with functional requirements, which define specific behaviours or functions of the system. Not functional requirements can be divided into two main categories:

- Execution qualities, such as security and usability, which are observable at run time;

- Evolution qualities, such as testability, maintainability, extensibility and scalability, which are embodied in the static structure of the software system.

Examples of relevant not-functional requirements include: accessibility, audit and control, availability (see service level agreement), backup, capacity (current and forecast), certification, compliance, configuration management, dependency on other parties , deployment, documentation, disaster recovery, efficiency (resource consumption for given load), effectiveness (resulting performance in relation to effort), emotional factors, environmental protection, escrow, exploitability, extensibility, failure management, legal and licensing issues, interoperability, maintainability, modifiability, network topology, open source, operability, performance/response time (performance engineering), platform compatibility, price, privacy, portability, quality (e.g. faults discovered, faults delivered, fault removal efficacy), recovery/recoverability (e.g. mean time to recovery - MTTR), reliability (e.g. mean time between failures - MTBF), reporting, resilience, resource constraints (processor speed, memory, disk space, network bandwidth, etc.), response time, robustness, safety, scalability (horizontal, vertical), security, standards compatibility, stability, supportability, testability, usability etc.

In the following a selection of not functional requirements which have emerged from the analysis and discussion of not functional issues related to the user requirements, functional requirements and CockpitCI vision presented above are provided.

There *will* be one CockpitCI tool for each CI (**NFR_1**). The CockpitCI tool of each Critical Infrastructure *shall* communicate with other CockpitCI tool deployed in different CIs by means of a Secure Mediation Network (**NFR_2**).

CockpitCI tool functionalities identified in the previous section, such as cyber detection, isolation and reaction, *shall* be implemented by means of a cyber detection layer and an online risk prediction layer (**NFR_3**).

In order to properly suggest the SCADA operator about reaction strategies to apply in case of cyber-attack in progress, the CockpitCI tool *shall* be an online (but not in-line) near real-time tool (**NFR_4**).

The CockpitCI tool *shall* be a CI independent tool (**NFR_5**). This means that it does not care about the type of data used by the specific CI it is linked to. All CI dependent raw data, coming from low level and high level equipment, *shall* be translated into shared data format by means of proper adaptors, i.e. SCADA adaptors and field adaptors (**NFR_6**).

Moreover, it *should* be possible to turn the CockpitCI tool ON or OFF with no effect on the normal SCADA system operation (**NFR_7**).This is a useful requirement from an engineering point of view, since it offers a quick recovery in the event that any security measure should affect the system operation. In general this requirement could be fulfilled in near real-time (e.g. for cyber detection), but in the case of an ongoing predetermined reaction this may be impossible or undesirable; in this case the tool *shall* be turned off only once the system has reached a safe state (**NFR_8**).

As mentioned in previous sections, it is important that the CockpitCI tool shall not alter or interfere with the normal operations of the SCADA system (UR_9), where the term “normal operations” refers to situations without cyber attacks. The CockpitCI tool should also not interfere with the normal flow of communication data between SCADA components (e.g. RTUs) and SCADA control center. In this context the CockpitCI tool *shall* not delay, block or alter the flow of packets sent from the SCADA control center to the RTU and vice-versa (**NFR_9**).

In order to guarantee the security of the CockpitCI tool, it *shall* be resistant to cyber-attacks in accordance with state-of-the-art security technologies (**NFR_10**).

The CockpitCI tool shall be a scalable solution (**NFR_11**).

The CockpitCI tool should cost reasonably (**NFR_12**).

the CockpitCI tool shall be effective both on new SCADA HW/SW as well as legacy SCADA HW/SW (**NFR_13**).

Finally, following requirements address the availability, documentation, reliability, response time, testability and usability properties of the CockpitCI tool.

The availability (see service level agreement) of the CockpitCI tool *should* be not lower than the availability of the interfacing systems and components (**NFR_14**).

CockpitCI tool development documentation *should* be adequate to perform an independent validation testing (**NFR_15**).

The CockpitCI tool response time *should* be adequate with the SCADA operator and cyber security staff reaction times in all the situations the tool is intended to support them (**NFR_16**).

The CockpitCI tool development process *should* grant the capability of the equipment to be tested against functional and not functional requirements, along the phase of validation testing (**NFR_17**).

Usability of CockpitCI tool by target user community: the CockpitCI tool *should* be easy to use and learn by SCADA operators and the cyber security support team (**NFR_18**).

Naturally, many not functional requirements are not appropriate in consideration of the prototypal nature of CockpitCI tool and the selection of adequate requirements for CockpitCI demonstration will mainly take into account functional requirements.

5.2.1 Not Functional requirements summary

The following table summarizes the identified and defined not functional system requirements.

Requirement id	Short description
NFR_1.	There *will* be one CockpitCI tool for each CI
NFR_2	The CockpitCI tool of each Critical Infrastructure *shall* communicate with other CockpitCI tool deployed in different CIs by means of a Secure Mediation Network
NFR_3	CockpitCI tool functionalities identified in the previous section, such as cyber detection, isolation and reaction, *shall* be implemented by means of a cyber detection layer and an online risk prediction layer
NFR_4	The CockpitCI tool *shall* be an online (but not in-line) near real-time tool
NFR_5	The CockpitCI tool *shall* be a CI independent tool
NFR_6	All CI dependent raw data, coming from low level and high level equipment, *shall* be translated into shared data format by means of proper adaptors, i.e. SCADA adaptors and field adaptors
NFR_7	It *should* be possible to turn the CockpitCI tool ON or OFF with no effect on the normal SCADA system operation
NFR_8	In the case of an ongoing predetermined reaction the CockpitCI tool *shall* be turned off only once the system has reached a safe state
NFR_9	The CockpitCI tool *shall* not delay, block or alter the flow of packets sent from the SCADA control centre to the RTU and vice-versa
NFR_10	The CockpitCI tool *shall* be highly resistant to cyber-attacks in accordance with state-of-the-art security technologies
NFR_11	The CockpitCI tool *shall* be a scalable solution
NFR_12	The CockpitCI tool *should* cost reasonably
NFR_13	The CockpitCI tool *shall* be effective both on new SCADA HW/SW as well as legacy SCADA HW/SW
NFR_14	The availability (see service level agreement) of the CockpitCI tool *should* be not lower than the availability of the interfacing systems and components
NFR_15	CockpitCI tool development documentation *should* be adequate to perform an independent validation testing
NFR_16	The CockpitCI tool response time *should* be adequate with the SCADA operator and cyber security staff reaction times in all the situations the tool is intended to support them

NFR_17	The CockpitCI tool development process *should* grant the capability of the equipment to be tested against functional and not functional requirements, along the phase of validation testing
NFR_18	Usability of CockpitCI tool by target user community: the CockpitCI tool *should* be easy to use and learn by SCADA operators and the cyber security support team

Table 3: Not functional system requirements

5.3 Requirements traceability matrix

In order to check that end-user requirements have been properly analyzed when deriving system requirements, the following table traces end-user requirements versus system requirements. All end-user requirements have been traced apart from UR_3, which is a generic desiderata which could be linked hopefully to many system requirements.

End-user requirement id	Short description	System requirement id
UR_1.	The CockpitCI tool *shall* improve the situational awareness and support the decision making capability of the SCADA operator in presence of cyber-attacks	FR_15; FR_16; FR_19; FR_22
UR_2	The CockpitCI tool *shall* improve the situational awareness and support the decision making of the cyber-security staff in presence of cyber-attacks	FR_13; FR_14; FR_17; FR_20
UR_3	The CockpitCI tool *shall* improve business continuity and resilience of services delivered to Critical Infrastructure customers in presence of cyber-attacks	Generic, not linked.
UR_4a	The Cockpit CI tool *shall* detect in near real-time cyber-attacks (including 0-days attacks) against the SCADA system	FR_1; FR_2; FR_5; FR_6; FR_7; FR_8; FR_11
UR_4b	The Cockpit CI tool *shall* isolate and react to cyber-attacks against the SCADA system	FR_23; FR_24; FR_25
UR_5	The detection, isolation and reaction strategies of the tool *should* minimize the perturbations on QoS to customers in terms of business continuity and resilience of services to CI customers	FR_26; NFR_4
UR_6	The CockpitCI tool *shall* identify the compromised sections of SCADA, ICT and in turn of the domain CI	FR_13
UR_7	The CockpitCI tool *shall* inform in real-time the security staff about the security state of the CI, the location and severity of the attack, action performed and the result of the correction action performed	FR_13; FR_17; FR_20
UR_8	Cancelled.	N.A.
UR_9	The CockpitCI tool *should* not alter or interfere with the normal operations of the SCADA system	NFR_9
UR_10	The CockpitCI tool *shall* not overload the SCADA operator with an excessive rate of false alarms	FR_3; FR_4

UR_11	The CockpitCI tool *shall* be a scalable solution	NFR_11
UR_12	The CockpitCI tool *should* cost reasonably	NFR_12
UR_13	the CockpitCI tool *shall* be effective both on new SCADA HW/SW as well as legacy SCADA HW/SW	NFR_13
UR_14	The CockpitCI tool *shall* be compatible and possibly integrable with other cyber security defence software	FR_10
UR_15	The CockpitCI tool *should* not use the SCADA communication infrastructure, but *should* provide its own communications means	NFR_9
UR_16	The CockpitCI tool *shall* provide an “intuitive” user interface that will provide the SCADA and security operators only with necessary information for decision making in uncertain situations	FR_19; FR_20
UR_17	The CockpitCI tool *should* also improve synergies between SCADA control and cyber security	FR_21
UR_18	The CockpitCI tool shall be configurable to a passive mode where attacks and suspicious traffic is detected and reported, but no active actions are taken.	FR_26

Table 4: Traceability matrix

6 System preliminary architecture and major components

In order to identify even the requirements referring to the principal architectural components, a preliminary study of a CockpitCI system architecture consistent with all the requirements identified so far, has been performed and is reported in this section. This architecture will be further detailed in the Task 5002.

The envisaged CockpitCI system architecture, in the case where two interdependent CIs are considered, is shown in Figure 3.

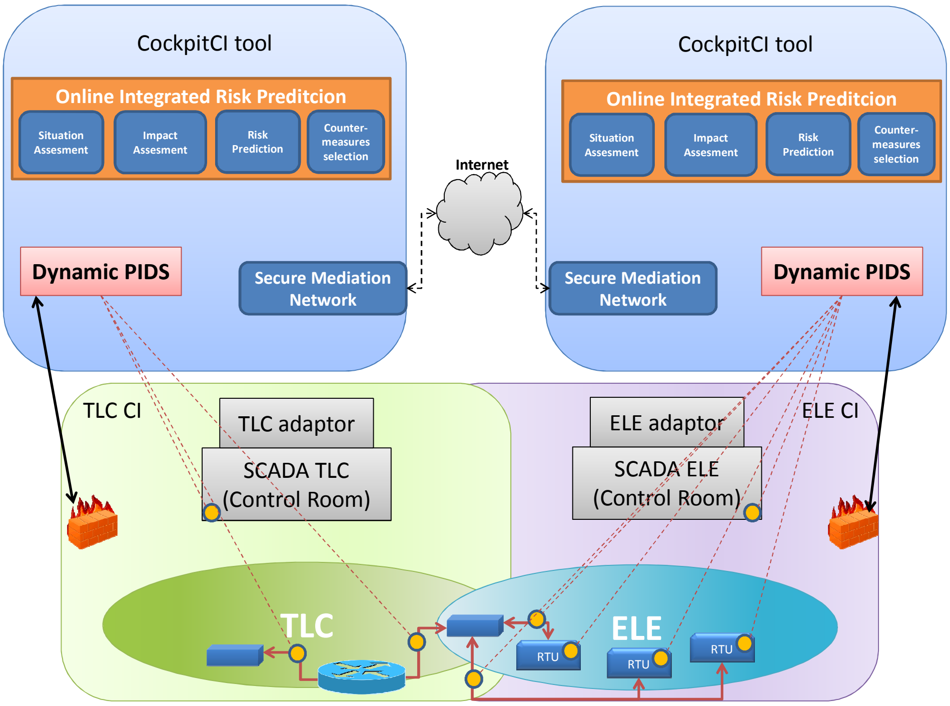


Figure 3: Simplified CockpitCI system architecture.

At the bottom of the figure, a conceptual and simplified illustration of the two CIs and of their interconnection is presented. In particular, for the sake of exposition, a telecommunication CI ("TLC" in the figure) and an electric distribution network ("ELE" in the figure) are considered. For each CI, both field elements (e.g. RTUs) and the SCADA control room ("SCADA ELE" and "SCADA TLC") are represented (the CockpitCI tool interacts both with field level devices and at control room level).

According to NFR_1, each CI has an associated CockpitCI tool (see the two rectangles at the top of the figure). Since, according to UR_11 and NFR_5, the CockpitCI tool must be a scalable and CI-technology independent solution, it is necessary to consider in the architecture also proper adaptors at the interface between the CockpitCI tool and the particular CI domain ("TLC adaptor" and "ELE adaptor" in the figure).

The CockpitCI tool architecture consists of three layers, namely detection layer, risk prediction layer and mediation layer. With reference to these layers, the main components of each CockpitCI tool are the following:

- Cyber **detection layer**, which will be a distributed layer including the cyber attack detection and classification functionalities, as well as the functionalities for providing reaction mechanisms at the local field level;

- An **online Integrated Risk Prediction (IRP)**, lying at risk prediction layer, which will merge relevant information, provide the situation awareness to operators and suggest appropriate reaction strategies;

- A **Secure Mediation Network**, lying at mediation layer, which will provide data exchange between the IRP and the detection layer, as well as data exchange between the considered CI and the neighbouring CIs.

As concerns the components lying at **Detection Layer,** they consist of (i) a centralized component, named **dynamic PIDS** (Perimeter Intrusion Detection System) (see figure 3), and (ii) a set of distributed **local detection agents** for intrusion detection at local level (the yellow dots in the figure). The local detection agents will be able to autonomously detect and (in some cases) react to local attacks, and will provide information to distributed IDS/IPS mechanisms. Detection agents, adaptors and extensions for system components will pervade CI's field and will be placed at the most critical sources of vulnerabilities, including RTUs and the main SCADA elements. The PIDS is a centralized component which correlates and aggregates the alerts received from the detection agents. Moreover, the PIDS has the capability to detect coordinated cyber-attacks, and to dynamically deploy containment or even preventive strategies of isolation (as an example, the PIDS could respond to detected threats by changing firewalls rules in order to redefine ICT system perimeters).

Information from local detection agents is gathered by adaptors (which perform all the needed operations in terms of filtering, aggregation, translation, etc.), and sent (in a technology independent format) to a centralized **on line Integrated Risk Prediction (IRP)** (at the top of the figure), which performs a situation assessment, computing the risk level associated to the current state of the CI, and evaluates the impact of cyber-attacks, suggesting also possible countermeasures. The IRP performs the above-mentioned situation assessment by properly analysing a *rich* input information merging both local field information (coming from the local CI Detection Layer) and global/remote information about the status of linked CIs, coming from linked IRPs. Notably, the connection between the IRP and the local detection layer is bidirectional in the sense that the results of IRP elaborations can be fed-back to the detection layer (to local detection agents and PIDS) in order to improve local detection and reaction capabilities. Hence, the output of the IRP will be provided both to control room operators and to the detection layer.

The secure and reliable communication between the detection layer and the IRP is assured by a **Secure Mediation Network**, which also supports the secure exchange of data between linked CIs. So doing, it is possible to combine local and global perspectives and obtain awareness at all the levels of the system. This is essential in view of the concept of interdependence introduced at the beginning.

The following of this section deals with the three main components of the architecture, i.e. the online Integrated Risk Prediction (see section 6.1), the components lying at Detection Layer (see section 6.2), and the Secure Mediation Network (see section 6.3). For each of these components, on the basis of a preliminary analysis of their functionalities, specific requirements, fully compatible with all the requirements identified so far, will be identified.

6.1 On-line Integrated Risk Prediction requirements

The on-line Integrated Risk Prediction (IRP) allows to enhance the level of awareness and to increase the fields' sensing and reaction capability considering both high and low level perspectives.

The Risk Prediction System alerts:

- the SCADA operator on the risk of degradation/loss of SCADA services and in turn of the degradation of the quality of services delivered to CI customers due to adverse events and cyber attacks;
- the cyber security staff along the detection, isolation and reaction phases of cyber attacks.

There are different indicators of the quality of services delivered to CI customers (i.e. the duration of service interruptions for customer for year, the number of long/short service interruptions for customer per year, etc.). A timely actuation of SCADA services, consequential to a permanent failure of the CI, reduces the CI outage duration and then contributes to keep indicators of quality of service to customers within prefixed values. On the contrary a delayed actuation of SCADA services may get such indicators worse.

The Integrated Risk Prediction is a tool (IRP tool) devoted to perform a prediction on the state of the whole system, basing its prediction both on the specific data of the field where the predictor is attested and on the output of predictions received by other Integrated Risk Prediction tools. The Integrated Risk Prediction is capable to influence the fields' equipment by means of suitable reaction strategies, commands and policies.

IRP tool requirements will account and will be compatible with the requirements of Secure Mediation Network and of the cyber detection layer.

Functional and not functional requirements of IRP tool shall be identified in an incremental fashion along CockpitCI project development and especially in the course of Task 4001 (On Line Integrated Risk Prediction requirements and design). In the following a minimum starting set is provided.

The on-line IRP tool requirements will be identified starting from the requirements of the MICIE risk prediction tool (see [13] and [14]). These requirements are properly adapted and extended to comply with the CockpitCI scenario discussed so far.

There *shall* be one IRP tool for each CI (**IRP_1**), typically installed in the SCADA Control Centre.

The CockpitCI IRP tool *shall* extend the level of awareness achieved in MICIE, exploiting field and SCADA level information and information coming from the Detection layer (**IRP_2**).

The IRP tool *shall* be able to provide the SCADA operator and cyber security staff with a near real-time risk-level assessment of QoS delivered to CI customers in presence of adverse events including cyber attacks on SCADA and ICT network (**IRP_3**).

The IRP tool *shall* employ in near real-time models which are able to predict the QoS delivered by SCADA systems and interconnected Telecommunication networks under cyber attacks (**IRP_4**).

The IRP tool *could* provide the probable cause which lies behind the observed situation (**IRP_5**).

The IRP tool *shall* provide warnings and suggest reaction strategies to the SCADA and/or cyber security operators (**IRP_6**).

The IRP tool *shall* also send alerts to fields equipment in order to support local containment and reaction strategies (**IRP_7**).

The IRP *shall* exploit models of SCADA systems under cyber-attacks, and their interdependencies with other CIs (**IRP_8**).

The IRP *shall* be based on the status of its own SCADA and ICT network and on the status of SCADA and ICT of the interconnected CIs, managing information coming from IRPs installed in other CIs (**IRP_9**).

In order to guarantee a proper functioning of the IRP, it is fundamental that information is readily updated: the IRP tool *shall* obtain updated information from the underlying CI, and from the IRP tools of the interconnected CIs (**IRP_10**). Clearly, a trade-off between accuracy and complexity arises.

IRP operations *could* be influenced also by external cyber security institutional entities, e.g. CERT (**IRP_11**).

The IRP tool *shall* keep to a minimum the impact on the CI's communication network (**IRP_12**)

Information shared between the different prediction tools *shall* be aligned (i.e. predictions shall rely on updated information, both local and coming from external interdependent CIs), in order to allow a proper functioning of the IRP tool (**IRP_13**).

The IRP tool *shall* provide an "intuitive" interface to SCADA operators (**IRP_14**).

6.1.1 On-line integrated risk prediction requirements summary

The following table summarizes the on-line integrated risk prediction tool requirements identified and proposed in this section.

Requirement id	**Short description**
IRP_1.	There *shall* be one IRP tool for each CI
IRP_2	The CockpitCI IRP tool *shall* extend the level of awareness achieved in MICIE, exploiting field and SCADA level information and information coming from the Detection layer
IRP_3	The IRP tool *shall* be able to provide the SCADA operator and cyber security staff with a near real-time risk-level assessment of QoS delivered to CI customers in presence of adverse events including cyber attacks on SCADA and ICT network
IRP_4	The IRP tool *shall* employ in near real-time models which are able to predict the QoS delivered by SCADA systems and interconnected Telecommunication networks under cyber attacks
IRP_5	The IRP tool *could* provide the probable cause which lies behind the observed situation
IRP_6	The IRP tool *shall* provide warnings and suggest reaction strategies to the SCADA and/or security operators
IRP_7	The IRP tool *shall* also send alerts to fields equipment in order to support local containment and reaction strategies

IRP_8	The IRP *shall* exploit models of SCADA systems under cyber-attacks, and their interdependencies with other CIs
IRP_9	The IRP *shall* be based on the status of its own SCADA and ICT network and on the status of SCADA and ICT of the interconnected CI, managing information coming from IRP installed in other CI
IRP_10	The IRP tool *shall* obtain updated information from the underlying CI, and from the IRP tools of the interconnected CIs
IRP_11	The IRP operations *could* be influenced also by external cyber security institutional entities, e.g. CERT
IRP_12	The IRP tool *shall* keep to a minimum the impact on the CI's communication network
IRP_13	Information shared between the different prediction tools *shall* be aligned (i.e. predictions shall rely on updated information, both local and coming from external interdependent CIs), in order to allow a proper functioning of the IRP tool
IRP_14	The IRP tool *shall* provide an "intuitive" interface to SCADA operators

Table 5: CockpitCI Integrated Risk Prediction (IRP) tool requirements

6.2 Detection Layer Requirements

In Section 5.1.1 the main requirements of the Detection Layer have been identified. In this section such requirements will be re-examined and further detailed, if possible, or simply restated. In particular requirement FR_1 asserts: "The cyber detection layer *shall* detect cyber-attacks". In this context it is important to give a formal definition of what is intended to be a cyber attack and how it has to be represented in the CockpitCI tool.

In particular, the representation of cyber attacks, in the CockpitCI framework, must be flexible enough to handle a wide array of situations – from clearly identifiable and traceable attacks to fuzzy signs of anomaly possibly induced by on-going attacks. The exact nature of this representation will be further detailed in WP3000. Nevertheless, it is already possible to provide a few hinting guidelines:

- In general, the Intrusion Detection System shall generate and handle security events.
- Security events correspond to events that might be potentially relevant, from a cyber security point of view.
- Some security events will be generated directly by local components in the detection layer (e.g. Host IDS or Network IDS sources), while other security events will result from the correlation of other security events.
- Correlation takes place at multiple levels of the platform, filtering out less relevant events and producing new, higher level, composite security events.
- Simple and composite security events will represent symptoms of possible attacks (e.g. suspicious network traffic, suspicious SCADA commands, abnormal traffic patterns, etc.).
- The analysis of these symptoms will ultimately lead, based on user-definable thresholds, to the release of security alarms to other components of the CockpitCI platform (such as the Risk Prediction Tool and the IT team). These alarms represent possible cyber attacks, with variable confidence level (from almost certain cyber attacks to situations where the system cannot distinguish a simple malfunction from an intentional attack). These alarms will also, whenever feasible, identify the nature of the attack and the CI components which are/may become compromised by the attack.

The requirements of the Detection layer will be developed in detail in Task 3001. In this paragraph the main high level system requirements which are relative to this layer are captured and a step forward in the understanding of such requirements is performed. The CockpitCI Detection Layer represents a valid improvement for extending the global awareness on the CI's state. The detection layer system can be split into two cooperating subsystems:

- Distributed system of detection agents and field adaptors, including agents, adaptors and extensions for existing system components (i.e., RTUs), as well as specialized network probes and honeypots to be added to the network.
- A centralized Perimeter Intrusion Detection System (PIDS), performing many of the tasks traditionally associated with a Distributed Intrusion Detection System. The PIDS is a centralized component which correlates and aggregates the alerts received from the detection agents. Moreover, the PIDS is able to deploy prevention strategies of isolation on the basis of advanced techniques of cyber-attack detection. Such techniques work on metadata, i.e. data translated to a common format, provided by different CockpitCI system components (IRP, field adaptors, DB of system metadata).

The Detection Layer requirements reported in the following derive from the concepts discussed so far and are consistent with the above-mentioned architecture outline.

The Detection Layer shall detect cyber attacks belonging to the classes listed in paragraph 3.2 (**DL_1**).

The Detection Layer should be capable to detect cyber-attacks before they affect the SCADA system (**DL_2**).

The Detection Layer shall provide near real-time monitoring of the area of interest (**DL_3**).

The Detection Layer *shall* identify the type of cyber-attack (**DL_4**).

The Detection Layer *shall* be able to detect cyber attacks by integrating classical approaches (e.g. signature based, classic anomaly-based detection and event correlation) with novel detection mechanisms based on adaptive machine learning and aggressive usage of topology and system-specific detection mechanisms (**DL_5**).

In order to take into account the different zones in which the SCADA system can be segmented (field, SCADA, corporate network) and the different requirements of each in terms of detection, correlation and reaction strategies, the architecture of the detection layer *should* adopt a multi-zone architecture (**DL_6**).

The architecture of the Detection Layer *should* adopt a multilevel correlation structure (**DL_7**).

In order to take advantage of the fact that control systems tend to be simpler than enterprise networks and tend to have traffic patterns that change much more slowly than do communication patterns in enterprise networks, the detection layer *shall* be able to detect anomalies in the information exchanged between SCADA control system and RTUs (**DL_8**).

The Detection Layer *shall* exploit local detection mechanisms (able to function autonomously on each component) and coordinated detection mechanisms, such as PIDS, for multi-dimensional distributed IDS (**DL_9**).

CockpitCI *shall* provide a Perimeter Intrusion Detection System (PIDS), able to detect CI scale cyber-attacks, and deploy prevention strategies of isolation (**DL_10**).

The Detection Layer *shall* extend the global awareness achieved with respect to the one achieved with the only IRP (**DL_11**).

The Detection Layer shall detect anomalies and deviations of the major functionalities of the SCADA system on the basis of metadata that are typical of a safe state CI. (**DL_12**).

The Detection Layer *shall* reduce the number of false positives and false negatives by means of advanced detection techniques and by providing the capability to tune the instrument to the desired level of false alarms performance (**DL_13**).

The PIDS *shall* use the secure mediation network component to transmit detection information to the IRP (**DL_14**). Such information will influence the cyber risk prediction.

Raw data generated by local detection agents *shall* be translated into CI independent metadata by means of proper field adaptors (**DL_15**).

Local Detection agents *shall* perform packet sniffing on the CI network (**DL_16**) in order to identify attack situations.

Local detection agents *shall* be able to detect localized security attacks (**DL_17**) and suggest the proper reaction (**DL_18**).

PIDS operations *shall* be also influenced by the following system information: system topology, system inventories with detailed information about each component, roles and policies applicable to system components, trust and reputation estimators for system components (**DL_19**).

The Detection Layer functionalities should account the pre-existent security policies, strategies and solutions of SCADA system and enterprise network as identified in the reference Scenario **(DL_20)**.

The Detection Layer *shall* provide an “intuitive” interface to security staff (**DL_21**).

6.2.1 Detection Layer requirements summary

The following table summarizes the detection layer requirements identified and proposed in this section.

Requirement id	**Short description**
DL_1	The Detection Layer shall detect cyber attacks belonging to the classes listed in paragraph 3.2.
DL_2	The Detection Layer *should* be capable to detect cyber-attacks before they affect the SCADA system
DL_3	The Detection Layer shall provide near real-time monitoring of the area of interest.
DL_4	The Detection Layer *shall* identify the type of cyber-attack
DL_5	The Detection Layer *shall* be able to detect cyber attacks by integrating classical approaches with novel detection mechanisms based on adaptive machine learning and topology
DL _6	The architecture of the detection layer *should* adopt a multi-zone architecture
DL _7	The architecture of the Detection Layer *should* adopt a multilevel correlation structure

DL _8	The Detection Layer *shall* be able to detect anomalies in the information exchanged between SCADA control system and RTUs
DL _9	The Detection Layer *shall* exploit local detection mechanisms, and coordinated detection mechanisms, such as PIDS
DL _10	CockpitCI *shall* provide a Perimeter Intrusion Detection System (PIDS), able to detect CI scale cyber-attacks, and deploy prevention strategies of isolation
DL _11	The Detection Layer *shall* extend the global awareness achieved with respect to the one achieved with the only IRP
DL _12	The Detection Layer *shall* detect anomalies and deviations of the major functionalities of the SCADA system on the basis of metadata that are typical of a safe state CI
DL _13	The Detection Layer *shall* reduce the number of false positives and false negatives by means of advanced detection techniques and by providing the capability to tune the instrument to the desired level of false alarms performance
DL_14	The PIDS *shall* use the secure mediation network component to transmit detection information to the IRP
DL_15	Raw data generated by local detection agents *shall* be translated into CI independent metadata by means of proper field adaptors
DL_16	Local Detection agents *shall* perform packet sniffing on the CI network
DL_17	Local detection agents *shall* be able to detect localized security attacks
DL_18	Local detection agents *shall* be able to suggest the proper reaction
DL_19	PIDS operations *shall* be also influenced by the following system information: system topology, system inventories with detailed information about each component, roles and policies applicable to system components, trust and reputation estimators for system components
DL _20	The Detection Layer functionalities should account the pre-existent security policies, strategies and solutions of SCADA system and enterprise network as identified in the reference Scenario
DL_21	The Detection Layer *shall* provide an “intuitive” interface to security staff

Table 6: Detection Layer requirements

6.3 Secure Mediation Network requirements

The Secure Mediation Network is a main element of the CockpitCI system which allows communication between main CockpitCI components. A key component of the Secure Mediation Network will be the Secure Mediation Gateway (SMGW): each CI will be equipped with one SMGW which will allow near real-time exchange of information between the Detection Layer and the IRP of the considered CI, as well as the exchange of information among the considered CI and the neighbouring CIs.

The Secure Mediation Network requirements reported in the following derive from the concepts discussed so far and are consistent with the above-mentioned architecture outline.

The Secure Mediation Network *shall* provide near real-time secure, reliable and available data exchange between the Detection Layer and the IRP, as well as among different CIs (**SMN_1**).

The Secure Mediation Network *shall* interface with the detection layer (**SMN_2**).

The Secure Mediation Network *shall* interface with the prediction tool (**SMN_3**).

The Secure Mediation Network *shall* interface with external peer Secure Mediation Networks through an Internet connection (**SMN_4**).

The Secure Mediation Network *shall* support non real-time exchange of other kinds of information among CIs, e.g. best practice and past experience (**SMN_5**).

The Secure Mediation Network *shall* acquire CI independent metadata from SCADA adaptors (**SMN_6**).

The Secure Mediation Network (SMN) *shall* store information obtained by all interfaced components (PIDS, SCADA adaptors, local IRP, peer SMGWs) in a dedicated database (**SMN_7**).

A specific framework *shall* be included in the Secure Mediation Network in order to allow local CockpitCI components and external SMGWs to retrieve metadata useful for their purposes(**SMN_8**)

The Secure Mediation Network *shall* perform information discovery at peer SMGWs to retrieve state information of interdependent CIs (**SMN_9**).

All ingoing and outgoing connections of the Secure Mediation Network *shall* be secure connections (**SMN_10**).

The Secure Mediation Network *shall* disclose stored global awareness metadata of the local CI, to authorized subscribers, i.e. other SMGWs (**SMN_11**).

The Secure Mediation Network *shall* accept subscriptions from peer SMGWs to be notified when updated metadata is available (**SMN_12**).

The Secure Mediation Network *shall* perform client authentication on the basis of client profiles and certificates (**SMN_13**).

The Secure Mediation Network *shall* perform security auditing (**SMN_14**).

In order to guarantee a reliable and effective risk prediction, the Secure Mediation Network *shall* keep synchronized with remote CIs' metadata. (**SMN_15**).

In addition the Secure Mediation Network *shall* provide a management interface allowing a certain degree of security and policies configuration, accordingly with the following requirements (**SMN_16**).

The Secure Mediation Network *should* provide the possibility to define who and in which way can access a certain piece of information (**SMN_17**).

The Secure Mediation Network *should* provide the possibility to define trust relations between different CIs (**SMN_18**).

The Secure Mediation Network *should* enforce different communications protocols/technologies in each particular context (**SMN_19**).

The Secure Mediation Network *should* enforce Service Level Agreements (SLA) or Service Level Specifications (SLS) between CIs(**SMN_20**).

6.3.1 Secure mediation network requirements summary

The following table summarizes the Secure Mediation Network requirements identified in this section.

Requirement id	Short description
SMN_1.	The Secure Mediation Network *shall* provide near real-time secure, reliable and available data exchange between the Detection Layer and the IRP, as well as among different CIs
SMN_2	The Secure Mediation Network *shall* interface with the detection layer
SMN_3	The Secure Mediation Network *shall* interface with the prediction tool
SMN_4	The Secure Mediation Network *shall* interface with external peer Secure Mediation Networks through an Internet connection
SMN_5	The Secure Mediation Network *shall* support non real-time exchange of other kinds of information among CIs
SMN_6	The Secure Mediation Network *shall* acquire CI independent metadata from SCADA adaptors
SMN_7	The Secure Mediation Network *shall* store information obtained by all interfaced components in a dedicated database
SMN_8	A specific framework *shall* be included in the Secure Mediation Network in order to allow local CockpitCI components and external SMGWs to retrieve metadata useful for their purposes
SMN_9	The Secure Mediation Network *shall* perform information discovery at peer SMGWs to retrieve state information of interdependent CIs
SMN_10	All ingoing and outgoing connections of the Secure Mediation Network *shall* be secure connections
SMN_11	The Secure Mediation Network *shall* disclose stored global awareness metadata of the local CI, to authorized subscribers, i.e. other SMGWs
SMN_12	The Secure Mediation Network *shall* accept subscriptions from peer SMGWs to be notified when updated metadata is available
SMN_13	The Secure Mediation Network *shall* perform client authentication on the basis of client profiles and certificates
SMN_14	The Secure Mediation Network *shall* perform security auditing
SMN_15	In order to guarantee a reliable and effective risk prediction, the Secure Mediation Network *shall* keep synchronized with remote CIs' metadata
SMN_16	The Secure Mediation Network *shall* provide a management interface allowing a certain degree of security and policies configuration
SMN_17	The Secure Mediation Network *should* provide the possibility to define who and in which

	way can access a certain piece of information
SMN_18	The Secure Mediation Network *should* provide the possibility to define trust relations between different CIs
SMN_19	The Secure Mediation Network *should* enforce different communications protocols/technologies in each particular context
SMN_20	The Secure Mediation Network *should* enforce Service Level Agreements (SLA) or Service Level Specifications (SLS) between CIs

Table 7: Secure Mediation Network requirements

7 Conclusions

This deliverable has identified the main set of requirements of the CockpitCI tool and it represents the starting point of the architectural design phase of the project (Task 5002, System Architecture Design). System requirements will be further discussed, detailed and refined in subsequent tasks (e.g. Task 4001 for the requirements and design of the integrated risk prediction tool and Task 3001 for the requirements and design of the analysis and detection layer).

The deliverable provides in sequence the vision of the Consortium, the objectives which stem from that vision and the end-user perspective, which has emerged from discussions involving the end-users and from the end-user questionnaire, which was prepared to orient the specification and design of the CockpitCI tool on specific issues. All this has provided the input for the system requirements definition phase.

In the requirement definition phase the approach followed has been to aim at identifying all possible and significant requirements which could shed light also on design, architectural and other pertinent issues in the perspective of a practical implementation of the CockpitCI system. The requirements proposed in this document comprehend system functional and not functional requirements and architectural components specific requirements. Also end-user requirements have been taken into consideration, in order to develop a system realistically capable to add value to state of the art available tools.

Of course the CockpitCI *target reference architecture* and the CockpitCI system actually implemented for the final project demonstration will be a particularization to a *specific CockpitCI implementation scenario*. The CockpitCI system actually implemented for the project demonstrator will comply with a relevant subset of the identified requirements (i.e. requirements defined in Task 2002 – Reference Scenario, see deliverable D2.2 as stated in the project proposal [2]).

8 References

1. S. M. Rinaldi, J. P. Peerenboom, T. K. Kelly, *Identifying, understanding, and analyzing critical infrastructure interdependencies*, *Control Systems, IEEE*, vol.21, no.6, pp.11-25, Dec 2001, doi: 10.1109/37.969131.

2. CockpitCI Consortium, *Cybersecurity on SCADA: risk prediction, analysis and reaction tools for Critical Infrastructures,* Project Proposal, PART B*,* 2011*.*

3. R. Tsang, *Cyberthreats, Vulnerabilities and Attacks on SCADA Networks*, pp. 5–6, 2009. [Online]. Available at: http://gspp.berkeley.edu/iths/Tsang_SCADA%20Attacks.pdf

4. P. Sommerlad, *Reverse Proxy Patterns.* [Online]. Available at: http://hillside.net/europlop/HillsideEurope/Papers/EuroPLoP2003/2003_Sommerlad_ReverseProxyPatterns.pdf

5. R. Smith, *The reverse proxy vulnerability affecting Apache,* 2011, [Online]. Available at: http://www.thesecuritysamurai.com/2011/11/28/the-reverse-proxy-vulnerability-affecting-apache-by-rory-smith-soc-analyst/

6. P. Stavroulakis and M. Stamp, *Handbook of Information and Communication Security*, Springer-Heidelberg, vol.1, pp. 399-400, 2010.

7. US-CERT website, *Clientless SSL VPN products break web browser domain-based security models*, 2012. [Online]. Available at*: http://www.kb.cert.org/vuls/id/261869*

8. E. Duvelson*, Bridging the Gap between Legacy and Modern Substation Communications.*

9. ABB Switzerland Ltd, *SCADA over IP-based LAN-WAN connections*, 2005.

10. N. Fovino, A. Coletta and M. Masera*, Taxonomy of security solutions for the SCADA sector, ESCORTS Deliverable D22*, pp. 22-28, 2010.

11. MICIE Consortium, *Deliverable D 2.2.3 - Interdependency modelling framework, indicators and models - final report,* Dec. 2010. [Online]. Available at: http://www.micie.eu/documents/MICIE_D2.2.3.pdf

12. Wikipedia, The Free Encyclopedia, *ISO/IEC 9126 Software engineering — Product quality International Standard.* [Online]. Available at: http://en.wikipedia.org/wiki/ISO/IEC_9126

13. MICIE Consortium, *Deliverable D 3.1.2 - Refined interdependency metrics and indexes, for risk prediction formulation - final version*, June 2010. [Online]. Available at: http://www.micie.eu/documents/MICIE_D3.1.2.pdf

14. MICIE Consortium, *Deliverable D 3.2.2 – Common ontology and risk prediction algorithms – final report*, Nov. 2010. [Online]. Available at: http://www.micie.eu/documents/MICIE_D3.2.2.pdf

15. MICIE website. Available at: http://www.micie.eu/

16. *Advanced threats: the new world order*, RSA APT Summit Finding, October 2011.

17. North American Electric Reliability Council (NERC), Control Systems Security Working Group (CSSWG). Website available at: http://www.nerc.com/

18. http://www.fi-ppp-finseny.eu/
19. M. Masera, I. Nai Fovino, B. Vamanu. *ICT aspects of power systems and their security* administrative Arrangement TREN/08/S07.9052 CEIP.

Appendix A – End-User questionnaires

When dealing with complex systems protection, and particularly with SCADA-based system protection (i.e. protection of *critical* systems in which man-machine interaction plays a crucial role), it is fundamental that both stakeholder's and operators' perspectives and needs are adequately evaluated and taken into account. That is, the CockpitCI tool must be a solution accepted by stakeholders and "aware of" SCADA operators and security team knowledge and practice.

In that perspective, this Appendix presents an end-user questionnaire that has been submitted to the end-user partners involved in the project. The objective has been to receive and stimulate a feedback from end-users, which has been beneficial to reach a shared vision of CockpitCI system requirements between consortium partners, thus orienting the specification and design of the CockpitCI tool towards a solution that is both technically effective and as much "acceptable" as possible.

The questionnaire touches the main concepts that the CockpitCI project deals with, among which:

- The need for increasing both global awareness and local decision-making capability;
- The concept of "situational awareness", and its relevance to end-users;
- The need for bridging the SCADA operations with the cyber security domains;
- Role and extent of local reaction strategies;
- Impact of the CockpitCI tool on the SCADA system.

The following questions have been proposed to the end-users:

Question #1: Which are the main cyber vulnerabilities which should be handled in SCADA systems? Is the communication network the most vulnerable element of the SCADA system? Which are the security threats which should be addressed in the reference scenario?

Question #2: In the domain of Critical Infrastructures Protection, the areas of SCADA operations and cyber security are today handled separately. Is it convenient to try and augment the synergy/convergence between these two areas and between the SCADA and the Cyber Security Operator? What is the situation today and how can it be improved? Which information needs to be exchanged and for what purpose?

Question #3: Is there a need to raise the Situation Awareness of SCADA and Cyber Security operators? If yes, can you provide some practical examples?

Question #4: Do you think it would be profitable for your organization to participate to a public-private partnership that could improve cyber awareness and hence on-line risk assessment?

Question #5: The CockpitCI proposal talks about "reaction to cyber threats" and "to increase the intelligence at RTU level providing them with some form of self-healing and self-protection capabilities". Should the CockpitCI tool be allowed to automatically start a reaction? Should field equipment like RTUs allowed to start local automatic reactions? Is this unacceptable or acceptable in some situations?

Question #6: The CockpitCI proposal talks about "the need to consider both the global and local perspective" and also "increasing both global awareness and local decision-making capability". How should we put together the local (field level) and global (SCADA control centre) perspective?

Question #7: The impact of the CockpitCI tool on the SCADA system should obviously be minimized (in terms of possible degradation, latency, …). Is a "no impact" solution a mandatory requirement? If no, please explain what level of impact may be tolerated.

Question #8: Should the CockpitCI information flows share the SCADA communication infrastructure or should they use a separate communication infrastructure?

Question #9: Are there any features/requirements missing in the CockpitCI proposal which you would like the CockpitCI tool to provide?

Question #10: Who is the operator of the CockpitCI tool? The SCADA operator and/or the security operator?

The end-users of the project consortium have all answered to the proposed questionnaire. Their perspective is shown in following sub-sections:

- Appendix A.1 IEC;
- Appendix A.2 LYSE;
- Appendix A.3 TRANS;

Appendix A.1 IEC

1. Open questions

The objective of this questionnaire is to receive and stimulate a feedback from end-users which may be beneficial to orient the specification and design of the CockpitCI tool.

Q1. Which are the main cyber vulnerabilities which should be handled in SCADA systems? Is the communication network the most vulnerable element of the SCADA system?

Which are the security threats which should be addressed in the reference scenario?

a. *For main SCADA vulnerabilities, please refer to document [19]. We have more or less the same as in the document item 3.3*

b. *I think that all of the threats, except organizational like training, documentation and so on, could be addressed in the scenarios*

Q2. In the domain of Critical Infrastructures Protection, the areas of SCADA operations and cyber security are today handled separately. Is it convenient to try and augment the synergy/convergence between these two areas and between the SCADA and the Cyber Security Operator? What is the situation today and how can it be improved? Which information needs to be exchanged and for what purpose?

I think that the same situation will be in future. It will be 2 different teams with different goals (one is to operate the CI and another to prevent cyber attacks). I also think that the CI operator should receive as minimum as possible information about cyber attacks and this information should be displayed to him in terms of possible risks to operate the CI without degradation of the SLA. From the hand the data security team should receive all information about cyber attacks and possible threats to the SCADA system operation and some (only for information) possible threats to the CI operation.

Today we have physical and cyber protection of SCADA systems. The situation will be improved by installing cyber control centre and implementing risk assessment for different CI based on analysis of abnormal situations

Q3. Is there a need to raise the Situation Awareness of SCADA and Cyber Security operators? If yes, can you provide some practical examples?

Yes, see document [19]. The situation is the same.

Q4. Do you think it would be profitable for your organization to participate to a public-private partnership that could improve cyber awareness and hence on-line risk assessment?

If you mean to take part in the conferences and commissions then the answer is yes.

Q5. The CockpitCI proposal talks about “reaction to cyber threats” and “to increase the intelligence at RTU level providing them with some form of self-healing and self-protection capabilities”. Should the CockpitCI tool be allowed to automatically start a reaction? Should field equipment like RTUs allowed to start local automatic reactions? Is this unacceptable or acceptable in some situations?

From the point view of the CI operation, question Q5 is composed of two different questions.

The first question addresses the CockpitCI tool and our answer is: "The possibility shall exist and the choice will be done by SCADA / Security Operator. In situations preliminary chosen by Operator, automatically started reaction will be pre-admitted, the system will auto react and go to a failsafe predefined state"; this is acceptable because the operator may *choose if the tool will start automatically or not, if yes then the system will have this failsafe state.*

The second question is about RTU behaviour. It sounds good to provide the RTU with some additional self protection capabilities, yet we have no experience with automatic restart of RTUs and it seems dangerous because an external person could manage the RTU. On the other hand for the research project it should be checked and analyzed.

Q6.The CockpitCI proposal talks about "the need to consider both the global and local perspective" and also "increasing both global awareness and local decision-making capability". How should we put together the local (field level) and global (SCADA control centre) perspective?

It is very simple. CockpitCI should analyse the abnormal situation on all SCADA levels (Control centre, communication, and field (RTU)) and provide to its users appropriate information for making decisions. Local for security team to prevent specific attacks and global on SCADA level to understand the possible threats to the SLA.

Q7.The impact of the CockpitCI tool on the SCADA system should obviously be minimized (in terms of possible degradation, latency, …). Is a "no impact" solution a mandatory requirement? If no, please explain what level of impact may be tolerated.

See answer to item Q5.

Q8.Should the CockpitCI information flows share the SCADA communication infrastructure or should they use a separate communication infrastructure?

See answer to Q5. CockpitCI should not be connected to the communication of the operational SCADA.

Q9.Are there any features/requirements missing in the CockpitCI proposal which you would like the CockpitCI tool to provide?

Q10. Who is the operator of the CockpitCI tool? The SCADA operator and/or the security operator?

See answer to Q2.

2. CockpitCI User requirements

This part of the questionnaire will help us to assess the first definitions of end-user expectations about the future CockpitCI tool. You are invited at least to give your opinion on the requirements and to assess the level of the requirements in case of deployment of the CockpitCI tool in your own system

First definition of User Requirements					**Rating**		
ID	**Short description**	**Agree**	**Disagree**	**Please provide a short comment if you are not agree or if the formulation is not correct according to you**	**Mandatory**	**Important**	**Optional**
UR_01	The CockpitCI tool *shall* improve the situational awareness and support the decision making capability of the SCADA operator in presence of cyber-attacks	v					
UR_02	The CockpitCI tool *shall* improve the situational awareness and support the decision making of the cyber-security staff in presence of cyber-attacks	v					
UR_03	The CockpitCI tool *shall* improve business continuity and resilience of services delivered to Critical Infrastructure customers in presence of cyber-attacks	v		How could it be tested?			
UR_04	The Cockpit CI tool *shall* detect, isolate and react in near real-time to cyber-attacks (including 0-days attacks) against the SCADA system		v	I think that the CockpitCI system should be a decision making system and should not be connected to any CI equipment. If it is a decision making system, then how it could isolate and react to cyber attacks?			
UR_05	The detection, isolation and reaction strategies of the tool *should* minimize the perturbations on QoS to customers in terms of business continuity and resilience of services to CI customers		v	The same as in UR-03 and UR-04			
UR_06	The CockpitCI tool *shall* identify the compromised sections of SCADA, ICT and in turn of the domain CI		v				

First definition of User Requirements					**Rating**		
ID	**Short description**	**Agree**	**Disagree**	**Please provide a short comment if you are not agree or if the formulation is not correct according to you**	**Mandatory**	**Important**	**Optional**
UR_07	The CockpitCI tool *shall* inform in real time the security staff about security state of the CI, the domain location and severity of the attack, action performed and the result of the correction action performed	v					
UR_08	CockpitCI functionalities (detection of cyber-attacks, isolation and reaction strategies) *shall* account the reference scenario		v	It is not a requirement			
UR_09	The CockpitCI tool *should* not alter or interfere with the normal operations of the SCADA system	v					
UR_10	The CockpitCI tool *shall* not overload the SCADA operator with an excessive rate of false alarms	v		And will provide to the CI operator the information in terms of SLA possible threats			
UR_11	The CockpitCI tool *shall* be a scalable solution	v					
UR_12	The CockpitCI tool *should* cost reasonably		v	It is not a requirement in terms of the system and it could not be tested			
UR_13	the CockpitCI tool *shall* be effective both on new SCADA HW/SW as well as existing SCADA HW/SW	v		Existing SCADA			
UR_14	The CockpitCI tool *shall* be compatible and possibly integrable with other cyber security defence software		v	It should be a stand alone system not connected to any other system			
UR_15	The CockpitCI tool *should* not use the SCADA communication infrastructure, but *should* provide its own communications means	v					
UR_16	The CockpitCI tool *shall* provide an “intuitive” user interface that will provide the SCADA operator only with necessary information for decision making in uncertain situations	v					

First definition of User Requirements					Rating		
ID	**Short description**	**Agree**	**Disagree**	**Please provide a short comment if you are not agree or if the formulation is not correct according to you**	**Mandatory**	**Important**	**Optional**
UR_17	The CockpitCI tool *should* also improve synergies between SCADA control and cyber security		v	Not clear			

Appendix A.2 LYSE

1. Open questions

The objective of this questionnaire is to receive and stimulate a feedback from end-users which may be beneficial to orient the specification and design of the CockpitCI tool.

Q1. Which are the main cyber vulnerabilities which should be handled in SCADA systems? Is the communication network the most vulnerable element of the SCADA system?

Which are the security threats which should be addressed in the reference scenario?

The following threats to SCADA systems should be handled by the CockpitCI tool:

- *Attacks from the corporate network and the Internet.*
- *Attacks from the field network (i.e. CI communications network).*
- *Inside attacks from malware/viruses/worms etc.*

The SCADA field network is often distributed in areas outside the control of the power company, hence it is vulnerable. In addition, the past has shown that illegal code installed inside the SCADA network has a great damage potential, especially as the software components of SCADA systems are updated rarely and may suffer from vulnerabilities over a long period of time.

Q2. In the domain of Critical Infrastructures Protection, the areas of SCADA operations and cyber security are today handled separately. Is it convenient to try and augment the synergy/convergence between these two areas and between the SCADA and the Cyber Security Operator? What is the situation today and how can it be improved? Which information needs to be exchanged and for what purpose?

In our organization, Lyse, the security operator and the SCADA operator are cooperating to reduce cyber threats. The cyber security operator often has more knowledge on general threats and operating system vulnerabilities and the SCADA operator has more knowledge on SCADA vulnerabilities. This information should be exchanged efficiently between the two parties.

Q3. Is there a need to raise the Situation Awareness of SCADA and Cyber Security operators? If yes, can you provide some practical examples.

This area of security awareness is an important area to focus on, as it is an area where the investments are most likely to be most efficient in improving the cyber security of SCADA systems and CI. Security awareness training programs should be mandatory for SCADA operators on a regular basis.

Q4. Do you think it would be profitable for your organization to participate to a public-private partnership that could improve cyber awareness and hence on-line risk assessment?

Yes, definitely. I believe it could be profitable for our organization to participate to such a partnership. How profitable this partnership would be, depends of course on how much resources we have to invest and on the outcome of this partnership. There is an initiative from the Norwegian government to establish a powerCERT, a Computer Emergency Response Team for the Norwegian power companies. If established, this CERT may be operated by private or governmental companies.

Q5.The CockpitCI proposal talks about "reaction to cyber threats" and "to increase the intelligence at RTU level providing them with some form of self-healing and self-protection capabilities". Should the CockpitCI tool be allowed to automatically start a reaction? Should field equipment like RTUs allowed to start local automatic reactions? Is this unacceptable or acceptable in some situations?

If the CockpitCI tool is allowed to act as an active system that can start automatic reactions, the system must pass very strict testing and QA procedures, and possibly approvals by governmental authorities. In some extraordinary situations, however, it might be acceptable to let the field equipment to enter an "attack mode" and ignore further commands and stay in a predefined state for a period of time.

Q6.The CockpitCI proposal talks about "the need to consider both the global and local perspective" and also "increasing both global awareness and local decision-making capability". How should we put together the local (field level) and global (SCADA control centre) perspective?

One way of putting together this perspective could be to base local reactions on the global threat situation, as described in question 5 ("attack mode").

Q7.The impact of the CockpitCI tool on the SCADA system should obviously be minimized (in terms of possible degradation, latency, …). Is a "no impact" solution a mandatory requirement? If no, please explain what level of impact may be tolerated.

Inside the SCADA network (i.e. SCADA control centre) only a passive tool would be accepted to avoid introducing latency and blocking of legal traffic. In the communication lines between SCADA network and corporate network and between SCADA network and field networks, an active tool with IPS-functions could be accepted.

Q8.Should the CockpitCI information flows share the SCADA communication infrastructure or should they use a separate communication infrastructure?

An "out-of-band" communication path would be preferable.

Q9.Are there any features/requirements missing in the CockpitCI proposal which you would like the CockpitCI tool to provide?

In its "simplest" form, the CockpitCI tool could be some sort of Intrusion Detection System that is customized for CI SCADA systems. Most attacks start with a reconnaissance phase to gather information to use in further attacks, and an "early warning" tool that can warn of such attacks would be welcome. Some sort of black/white listing functions for ip addresses could also prove to be useful.

Q10. Who is the operator of the CockpitCI tool? The SCADA operator and/or the security operator?

As the tool may also operate on the corporate network and Internet accesses, I would say the security operator is the main operator of the tool.

2. CockpitCI User requirements

This part of the questionnaire will help us to assess the first definitions of end-user expectancies about the future CockpitCI tool. You are invited at least to give your opinion on the requirements and to assess the level of the requirements in case of deployment of the CockpitCI tool in your own system.

First definition of User Requirements					Rating		
ID	**Short description**	**Agree**	**Disagree**	**Please provide a short comment if you are not agree or if the formulation is not correct according to you**	**Mandatory**	**Important**	**Optional**
UR_01	The CockpitCI tool *shall* improve the situational awareness and support the decision making capability of the SCADA operator in presence of cyber-attacks		X	The SCADA operator could be warned about cyber-attacks, but he is not expected to take any action on his/her own in such situations.			X
UR_02	The CockpitCI tool *shall* improve the situational awareness and support the decision making of the cyber-security staff in presence of cyber-attacks	X				X	
UR_03	The CockpitCI tool *shall* improve business continuity and resilience of services delivered to Critical Infrastructure customers in presence of cyber-attacks	X				X	
UR_04	The Cockpit CI tool *shall* detect, isolate and react in near real-time to cyber-attacks (including 0-days attacks) against the SCADA system		X	Disagreement originates from the suggested zero-day attack protection. Zero-day attacks occur also during the vulnerability window that exists in the time between when a vulnerability is first exploited and when software developers start to develop a counter to that threat. To efficiently protect against such threats, the CockpitCI tool would have to be updated automatically via Internet on a frequent basis. This security feature is normally found on perimeter devices like IPS and may be omitted for a less complex design of the CockpitCI tool.		X	
UR_05	The detection, isolation and reaction strategies of the tool *should* minimize the perturbations on QoS to customers		X			X	

First definition of User Requirements					Rating		
ID	**Short description**	**Agree**	**Disagree**	**Please provide a short comment if you are not agree or if the formulation is not correct according to you**	**Mandatory**	**Important**	**Optional**
	in terms of business continuity and resilience of services to CI customers						
UR_06	The CockpitCI tool *shall* identify the compromised sections of SCADA, ICT and in turn of the domain CI	X					X
UR_07	The CockpitCI tool *shall* inform in real time the security staff about security state of the CI, the domain location and severity of the attack, action performed and the result of the correction action performed	X					X
UR_08	CockpitCI functionalities (detection of cyber-attacks, isolation and reaction strategies) *shall* account the reference scenario	X					X
UR_09	The CockpitCI tool *should* not alter or interfere with the normal operations of the SCADA system	X			X		
UR_10	The CockpitCI tool *shall* not overload the SCADA operator with an excessive rate of false alarms	X			X		
UR_11	The CockpitCI tool *shall* be a scalable solution	X			X		
UR_12	The CockpitCI tool *should* cost reasonably	X			X		
UR_13	the CockpitCI tool *shall* be effective both on new SCADA HW/SW as well as legacy SCADA HW/SW	X					X
UR_14	The CockpitCI tool *shall* be compatible and possibly integrable with other cyber security defence software	X					X
UR_15	The CockpitCI tool *should* not use the SCADA communication infrastructure, but *should* provide its own communications means	X					X

First definition of User Requirements					Rating		
ID	**Short description**	**Agree**	**Disagree**	**Please provide a short comment if you are not agree or if the formulation is not correct according to you**	**Mandatory**	**Important**	**Optional**
UR_16	The CockpitCI tool *shall* provide an "intuitive" user interface that will provide the SCADA operator only with necessary information for decision making in uncertain situations	X					X
UR_17	The CockpitCI tool *should* also improve synergies between SCADA control and cyber security	X				X	

You can also provide a new user requirement for CockpitCI to be online with the expectancies of your own business in the table below:

Proposition of User Requirements			Rating		
ID	**Short description**	**Expectancies covered by the UR and level of importance**	**Mandatory**	**Important**	**Optional**
UR_A	The CockpitCI tool *shall* be configurable to a passive mode where attacks and suspicious traffic is detected and reported, but no active actions are taken.		X		
UR_B	The CockpitCI tool *should* have an easy to use graphical user interface.				X

Appendix A.3 TRANS

Author	Version	Date
Task 5.1 Team	0.5	15/05/2012

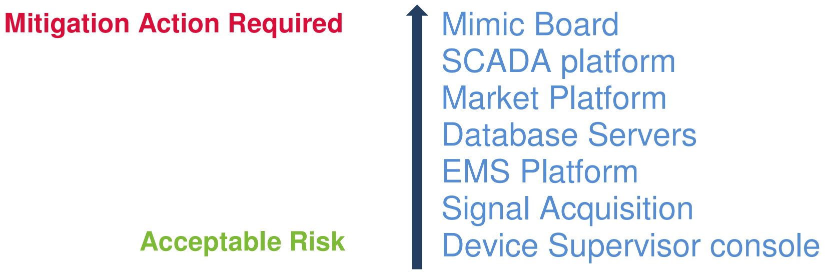
1. Open questions

The objective of this questionnaire is to receive and stimulate a feedback from end-users which may be beneficial to orient the specification and design of the CockpitCI tool.

Q1.Which are the main cyber vulnerabilities which should be handled in SCADA systems? Is the communication network the most vulnerable element of the SCADA system?

R: The main cyber vulnerabilities according of our internal security risk assessment on SCADA platform based on other project that was in Transelectrica:

- *High risks - Worms, viruses, Trojans, trapdoor, race condition, logic/time bomb, input validation failures, code injection, buffer overflow, bots*
- *Significant risks – Impersonation: water damaging, unauthorized removal of hardware, unauthorized access, unauthorized use of equipment, tampering with hardware, spear phishing, sever power lines, sever phone/ network circuits, sever of air-conditioning, position detection, destruction of hardware/ software, phishing, packet flood, malformed packets, key logger, infected memory device, dumpster diving, deception, corruption of data, arson*
- *Medium risks - Theft of media or documents, theft of laptop, retrieval of recycled or discarded media, fraudulent copying of software*
- *Components that have been considered in the risk assessment on Transelectrica SCADA platform (see the picture form Annex 1):*



Which are the security threats which should be addressed in the reference scenario?

R : For Transelectrica, considers that attacks and threats to control systems, the most common and dangerous threats could originate from our internal structures. The Transelectrica SCADA platform is centralized, collecting data on a national level through its own communication infrastructure and concentrates such data in Bucharest, where system servers process received information and forward them to Territorial Power Dispatchers /National Power Dispatchers in order to achieve the real time image of the local and national energetic status.

Q2. In the domain of Critical Infrastructures Protection, the areas of SCADA operations and cyber security are today handled separately. Is it convenient to try and augment the synergy/convergence between these two areas and between the SCADA and the Cyber Security Operator? What is the situation today and how can it be improved? Which information needs to be exchanged and for what purpose?

R : Operational personnel means the staff whose activity consists of operating electric installations by monitoring their running, direct parameter regulation and manoeuvres made into an installation or network area. Usually operational personnel are included in the organisational diagram of the managerial unit and perform their activity in the respective installations and network areas. Installations and equipment to be operated by a team are nominated under a decision from the managerial unit. Remote control (tele-control) is usually performed by the speciality operational control personnel from a dispatcher centre. The Transelectrica ICT operation is under the responsibility of a fully owned subsidiary, TELETRANS, which also incorporate the system operation team in charge of the Energy Management System (EMS)/SCADA system.

Q3. Is there a need to raise the Situation Awareness of SCADA and Cyber Security operators? If yes, can you provide some practical examples.

R : Yes. To raise the situation awareness of SCADA regarding cyber security is a necessity. In addition to technical countermeasures, Transelectrica puts in place organizational actions for fulfilling SCADA security requirements for example, the operating personnel are trained and provided with cyber security guidelines for EMS/SCADA system. Many cyber security countermeasures on SCADA system are under the responsibility of TELETRANS a Transelectrica subsidiary.

Operation informatics services offered by TELETRANS to Transelectrica are system maintenance and process monitoring for best operation. Therefore, TELETRANS ensures preventive or corrective maintenance services for the main critical importance information systems that provide the system operator functions, transport and those of the balancing market:

- *The EMS / SCADA system*
- *The Balancing Market system*
- *The neighboring countries real time data exchange system (ENTSO-E node)*
- *Visualization and monitoring systems*
- *Telemanaging systems (in deployment)*
- *SCADA system from the reengineering stations which also have the acquisition and remote functions*
- *The data acquisition data equipment (RTU)*

Among the system management and information process services, TELETRANS offers:

- *Solving and managing disturbances and support services in IT security for EMS/SCADA system.*
- *Database management and update, archive and plans saving, backup*

Additionally to the maintenance services, the TELETRANS team is prepared to bring added value to integrating the new command-control systems from the reengineering stations in the EMS/SCADA system.

Q4. Do you think it would be profitable for your organization to participate to a public-private partnership that could improve cyber awareness and hence on-line risk assessment?

R : The Transelectrica process control and its real time aspects regarding cyber security are thus considered through the acquisition system point of view. The manufacturer expertise in cyber security is the one of system and software integrator for Transelectrica EMS/SCADA system. The manufacturer of EMS/SCADA system and its expertise in cyber security is important for Transelectrica. The focus is more on delivery of intrinsic secure systems than on the cyber security environment where there are installed for operation. This doesn't mean that these aspects are not considered, especially in term of services, but that Transelectrica specifies in this domain should be expressed with the required information to reach a specific level operation.

Q5. The CockpitCI proposal talks about “reaction to cyber threats” and “to increase the intelligence at RTU level providing them with some form of self-healing and self-protection capabilities”. Should the CockpitCI tool be allowed to automatically start a reaction? Should field equipment like RTUs allowed to start local automatic reactions? Is this unacceptable or acceptable in some situations?

R: Transelectrica doesn't have evidences about effective cyber-attacks to the own SCADA platform. In general, SCADA platform and EMS platform of Transelectrica, seem to be well protected against attacks, but, after our security operator opinions, they are subject to some high risks due to malware and code attacks, which may determine major impacts on SCADA platform and EMS platform and so, they require at least a high protection level. Increasing the quality of controls and countermeasures like test, evaluation, monitoring and reporting, network configuration may be required to mitigate risks.

Q6. The CockpitCI proposal talks about “the need to consider both the global and local perspective” and also “increasing both global awareness and local decision-making capability”. How should we put together the local (field level) and global (SCADA control centre) perspective?

R : When we discuss about initiatives and the current security best practices, it was evident that decision maker, for example, Transelectrica like end-user, need evidence and the best available information on the security attributes -vulnerabilities, threats, attack mechanisms, countermeasures- for determining the best possible actions.

In general, the vendor of SCADA technologies possesses their laboratories for testing their equipment and validating their characteristics. But these tests typically treat the systems of the own manufacturer, and do not simulate the industrial operating platform. The thorough analysis of the security of SCADA would need the reproduction of the whole industrial setting, including the components being controlled, the interface of operators, and the policies of company regarding the networks and systems (e.g. access, maintenance, security).

Now, Transelectrica has no the experimental SCADA platform or any other technical possibility to determine the real existence and the severity of IT&C vulnerabilities for SCADA platform, and the effectiveness of the attacks that can exploit them and of the countermeasures for protecting them. Analytic approaches fall short of providing a complete view of the security attributes, and field data (although important) cannot *provide explanations (e.g. how representative are they of the situation of given architectures or technologies, etc.).*

Q7.The impact of the CockpitCI tool on the SCADA system should obviously be minimized (in terms of possible degradation, latency, …). Is a "no impact" solution a mandatory requirement? If no, please explain what level of impact may be tolerated.

R : In our opinion « no impact » is mandatory. The nature of the cyber security experiments in SCADA platform, is, not rarely, very invasive and disruptive. Conducing such tests in a production environment could cause unpredictable damages to the infrastructure itself that could be major for the availability of SCADA system that must be 99,99%.

Q8.Should the CockpitCI information flows share the SCADA communication infrastructure or should they use a separate communication infrastructure?

R : In our opinion CockpitCI information flows should use a separate communication infrastructure.

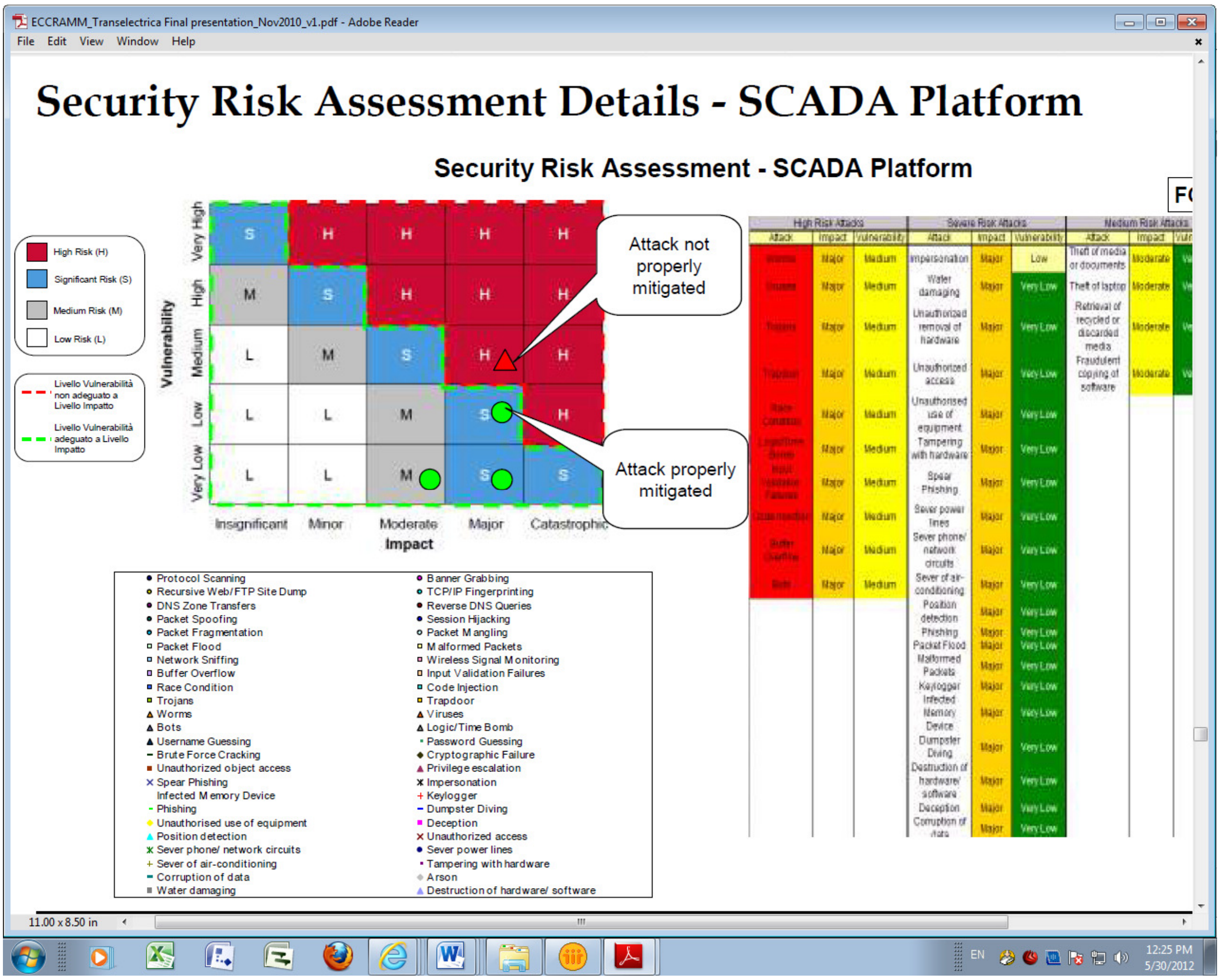
Q9.Are there any features/requirements missing in the CockpitCI proposal which you would like the CockpitCI tool to provide?

R : In this phase, we haven't any answer to this questions.

Q10. Who is the operator of the CockpitCI tool? The SCADA operator and/or the security operator?

R : In our opinion, the SCADA security operator will be able to use the CockpitCI tool, taking into account their experiences in IT&C Security areas.

ANNEX 1


ECCRAMM_Transelectrica Final presentation_Nov2010_v1.pdf - Adobe Reader
File Edit View Window Help
11.00 x 8.50 in
EN
12:25 PM
5/30/2012

Security Risk Assessment Details - SCADA Platform

Security Risk Assessment - SCADA Platform

- 🟥 High Risk (H)
- 🟦 Significant Risk (S)
- ⬜ Medium Risk (M)
- □ Low Risk (L)

- Livello Vulnerabilità non adeguato a Livello Impatto
- Livello Vulnerabilità adeguato a Livello Impatto

Vulnerability	Insignificant	Minor	Moderate	Major	Catastrophic
Very High	S	H	H	H	H
High	M	S	H	H	H
Medium	L	M	S	H	H
Low	L	L	M	S	H
Very Low	L	L	M	S	S
	Impact				

Attack not properly mitigated

Attack properly mitigated

● Protocol Scanning	● Banner Grabbing
● Recursive Web/FTP Site Dump	● TCP/IP Fingerprinting
● DNS Zone Transfers	● Reverse DNS Queries
● Packet Spoofing	● Session Hijacking
● Packet Fragmentation	○ Packet M angling
□ Packet Flood	□ M alformed Packets
□ Network Sniffing	□ Wireless Signal M onitoring
□ Buffer Overflow	□ Input Validation Failures
■ Race Condition	□ Code Injection
□ Trojans	□ Trapdoor
▲ Worms	▲ Viruses
▲ Bots	▲ Logic/Time Bomb
▲ Username Guessing	▪ Password Guessing
− Brute Force Cracking	◆ Cryptographic Failure
■ Unauthorized object access	▲ Privilege escalation
× Spear Phishing	✱ Impersonation
Infected M emory Device	+ Keylogger
− Phishing	− Dumpster Diving
◆ Unauthorised use of equipment	■ Deception
▲ Position detection	× Unauthorized access
✱ Sever phone/ network circuits	● Sever power lines
+ Sever of air-conditioning	▪ Tampering with hardware
− Corruption of data	◆ Arson
■ Water damaging	▲ Destruction of hardware/ software

High Risk Attacks			Severe Risk Attacks			Medium Risk Attacks		
Attack	Impact	Vulnerability	Attack	Impact	Vulnerability	Attack	Impact	Vuln
Worms	Major	Medium	Impersonation	Major	Low	Theft of media or documents	Moderate	Ve
Viruses	Major	Medium	Water damaging	Major	Very Low	Theft of laptop	Moderate	Ve
Trojans	Major	Medium	Unauthorized removal of hardware	Major	Very Low	Retrieval of recycled or discarded media	Moderate	Ve
Trapdoor	Major	Medium	Unauthorized access	Major	Very Low	Fraudulent copying of software	Moderate	Ve
Race Condition	Major	Medium	Unauthorised use of equipment	Major	Very Low			
Logic/Time Bomb	Major	Medium	Tampering with hardware	Major	Very Low			
Input Validation Failures	Major	Medium	Spear Phishing	Major	Very Low			
Code Injection	Major	Medium	Sever power lines	Major	Very Low			
Buffer Overflow	Major	Medium	Sever phone/ network circuits	Major	Very Low			
Bots	Major	Medium	Sever of air-conditioning	Major	Very Low			
			Position detection	Major	Very Low			
			Phishing	Major	Very Low			
			Packet Flood	Major	Very Low			
			Malformed Packets	Major	Very Low			
			Keylogger	Major	Very Low			
			Infected Memory Device	Major	Very Low			
			Dumpster Diving	Major	Very Low			
			Destruction of hardware/ software	Major	Very Low			
			Deception	Major	Very Low			
			Corruption of data	Major	Very Low			

FC