FP7-SEC-2011-1 Project 285647

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

D5.2- CockpitCI System architecture design

General information	
Submission date	21 December 2012
Dissemination level	Public
State	Final Version
Work package	WP5000 - System Development and Integration
Task	Task 5002: CockpitCI System architecture design
Delivery date	31 December 2012

Editors

Name	Organisation
Pietro Ricci	SELEX-SI

Authors

Name	Organisation
Antonio Graziano, Pietro Ricci, Alessio Liburdi, Federico De Padova	SELEX-SI
Donato Macone, Francesco Liberati, Andrea Simeoni, Andrea Simeoni, Francesco Delli Priscoli. Roberto Cusani, Manlio Proia, Vincenzo Suraci and all the UoR-CRAT team	CRAT
Lasith Yasakethu	SURREY
Matthieu Aubigny	ITRUST
Stefano Panzieri	ROMA 3
Tania Roman	TRANS
Are Kvinnesland	LYSE

Reviewers

Name	Organisation	Approval Date
Moussa Ouedraogo	CRPHT	21 December 2012

Executive Summary

Table of contents

List of figures

List of tables

1 Introduction

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

The FP7 MICIE project (“Tool for systemic risk analysis and secure mediation of data exchanged across linked CI information infrastructures”, EU-FP7-ICT-SEC-2007) has proved that increasing cooperation among infrastructures increases their level of service and predictive capability, but this is not enough to effectively counteract threats such as cyber attacks. Cyber threats cannot be addressed like any other failure or fault, e.g. in terms of the effects they induce on the rest of the system, because in this way the Operator response would always be lagging behind the cyber threat. Cyber threats need to be engaged as cyber threats, trying to identify the type of attack and its likely propagation and enforcing the appropriate countermeasures in order to better contain the threat and limit the scope of its impact. Cyber attacks could be performed blocking communication from central SCADA to local equipments or inserting fake commands/measurements in the SCADA-field equipment communications (as happened with the STUXNET worm).

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

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

The CockpitCI project aims on one hand to continue the work done in MICIE by refining and updating the on-line Risk Predictor deployed in the SCADA centre and sharing real-time information among CI owners, on the other hand to add cyber detection capabilities in order to get a broader perspective in terms of security, to identify in near real time the CI functionalities impacted by cyber-attacks and to assess the degradation of CI delivered services. CockpitCI aims to classify the associated risk level and activate a strategy of containment of the possible consequences of cyber-attacks together with the provision of some kind of intelligence to field equipment, allowing it to perform local decisions in order to self-identify and self-react to abnormal situations induced by cyber attacks.

The objective of this document is to design the overall CockpitCI system architecture in terms of system components, information flows, functional diagrams and interfaces among components. In order to address the concerns of those who are sceptical about automatic reaction mechanisms and doubt that CI operators will ever accept them, two different versions of the system architectures are investigated:

- a **basic architecture** where the system is basically a decision support tool, it operates in a purely passive (monitoring) mode and detects and reports attacks and suspicious traffic, but no automatic reaction mechanisms are envisaged. The basic architecture is also suited for legacy systems since it does not require any change or modification to the legacy SCADA system configuration.
- an **advanced architecture**, which is of course based on the same basic architecture and provides enhanced capabilities in terms of automatic reaction.

It is important to underline the fact that the interest for an automatic reaction capability arises from the consideration that mission critical applications should adhere to the graceful degradation principle and provide minimum acceptable levels of service even under active attacks and intrusions or if partially compromised. The idea is therefore to build an adaptive architecture which may, automatically or manually, reduce its signature and exposure to a minimum in presence of a cyber attack and then return to normality when the cyber alarm ceases. In addition during normal operation, parts of the system may be disconnected from the SCADA central control due to a cyber attack; the need arises for deploying intelligence at the local level so that these situation can be managed rather than leave isolated portions of the network in the hands of the attackers. The attacker may cause serious damage, from an economic and social point of view as well as a damage which may take several time to repair and restore. Inaction or late response are more detrimental than a predefined reaction capability, even though this increases the chance of false positives and therefore the fact that the reaction may be triggered off inappropriately.

The overall situation is characterized by significant uncertainty (uncertainty in the causes of the fault, in the characteristics and goals of the cyber attack, ...) and therefore risk must be handled and proper risk evaluation should be performed.

The specific details of components such as the Cyber Analysis and Detection Layer, which is responsible for cyber detection, and the Integrated Risk Prediction, which is responsible for risk assessment, are provided in specific deliverables, currently in their preliminary version ([2],[6]). The objective of this document is therefore to provide a coherent picture of how the main components fit together and allow to reach the desired objectives of the project.

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 and a list of acronyms and symbols that recur in the document.

Section 2 provides a contextual system description. In particular the section contains the identification of system components process and a description of CockpitCI tool operative context.

Section 3 provides several system architectural products of the CockpitCI tool such as the information flows, system components description and system interfaces and design. The section contains functional scheme and diagrams which describe the system components behaviour. With reference to CockpitCI system design the section contains two configurations of the system: a basic one and an advanced one which include countermeasures and automatic reactions strategies. Section 4 provides the identification and the description of system interfaces existing among the CockpitCI tool main components. Section 5 addresses the tool interface (HMI) towards the SCADA and the ICT Operator and how the tool can support the coordination and collaboration among the Operators. Section 6 addresses the security issues of the CockpitCI tool and includes a preliminary security architecture. Finally section 7 provides conclusions.

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.
Cyber attack phase	One of the phases of a typical cyber attack: typical phases include reconnaissance, penetration, exploitation and conclusion.
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 Acronyms and Symbols

Acronym or symbols	Explanation
BEEP	Blocks Extensible Exchange Protocol
BMS	Backup Master Station
CERT	Computer Emergency Response Team
CI	Critical Infrastructure
CS	Control Systems
DB	Data Base
DL	Detection Layer
DMS	Distributed Monitoring System
DOS	Denial Of Service
DMZ	DeMilitarized Zone
EAL	Evaluation Assurance Level
ELE	Electric
EU	European Union
FSM	Field Security Manager
HIDS	Host Intrusion Detection System
HMI	Human-Machine Interface
HW	Hardware
I/O	Input/Output
ICS	Industrial Control System
ICT	Information and Communication Technology
IDMEF	Intrusion Detection Message Exchange Format
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
MSC	Message Sequence Chart
N.A.	Not Applicable
NIDS	Network Intrusion Detection System
OWASP	Open Web Application Security Project
PE	Personnel
PIDS	Perimeter Intrusion Detection System
PLC	Programmable Logic Controller
POC	Proof Of Concept
QoS	Quality of Service
RTU	Remote Terminal Unit
SCADA	Supervisory Control and Data Acquisition
SLA	Service Level Agreements
SMGW	Secure Mediation Gateway
SMN	Secure Mediation Network
SNMP	Simple Network Management Protocol
SSL	Secure Sockets Layer
SW	Software
TCP	Transmission Control Protocol
TLC	Telecommunications
UDP	User Datagram Protocol
US-CERT	United States- Computer Emergency Response Team
USB	Universal Serial Bus
VPN	Virtual Private Network

2 CockpitCI system overview

2.1 Identification of system components

The main functional requirements of the CockpitCI tool which have been identified in D5.1 are :

- Cyber Attack Detection, in order to detect cyber threats;
- Cyber Attack Identification, in order to identify the type of cyber threats, where applicable;
- 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;
- Secure Data Exchange, with neighbouring and interdependent CIs.

Starting from system requirements and functionalities, the main system components can be identified as a set of modules, each related to a subset of proper functions. Following this approach, three main CockpitCI modules have been identified:

- **Cyber Analysis and Detection Layer (DL)**
- **Integrated Risk Prediction (IRP)**
- **Secure Mediation Network (SMN)**

The main objective of the cyber detection layer is to detect in near real-time cyber-attacks in a monitored area of interest. For CockpitCI system, the monitored area embraces/includes the entire CI network.

The output of the DL feeds the IRP module whose primary scope is to support the decision making process. The Online Integrated Risk Prediction System, by considering both high and low level perspectives, enhances the global awareness and the fields' sensing and reaction capability.

Finally, the Secure Mediation Network is the fundamental component allowing secure and reliable exchange of data among the internal CockpitCI modules. Noteworthy, the SMN is designed also to support the secure and reliable exchange of information among linked CIs (via communication of peer SMNs), which is fundamental in view of the concept of CI interdependence.

The table below resumes the matching between functional requirements introduced in D5.1 and CockpitCI components.

Main functionalities	System Component
•Cyber Attack Detection, in order to detect cyber threats; •Cyber Attack Identification, in order to identify the type of cyber threats; •Enforce cyber countermeasures; •Provide local intelligence and reaction capabilities;	**Cyber Analysis and Detection Layer (DL)**
•Building Situation Awareness •Understand the current situation; •Predict the near term evolution of the situation; •Risk prediction; •Reaction; •Support the selection of appropriate countermeasures; •Trigger automatic reaction logics;	**Integrated Risk Prediction (IRP)**
Secure Data Exchange	**Secure Mediation Network (SMN)**

Table 2-1 CockpitCI functionalities versus system components

2.2 CockpitCI tool in context

A preliminary vision of the context in which the CockpitCI tool is going to operate is depicted in the following figure, which highlights the main components of the CockpitCI system and their interactions.

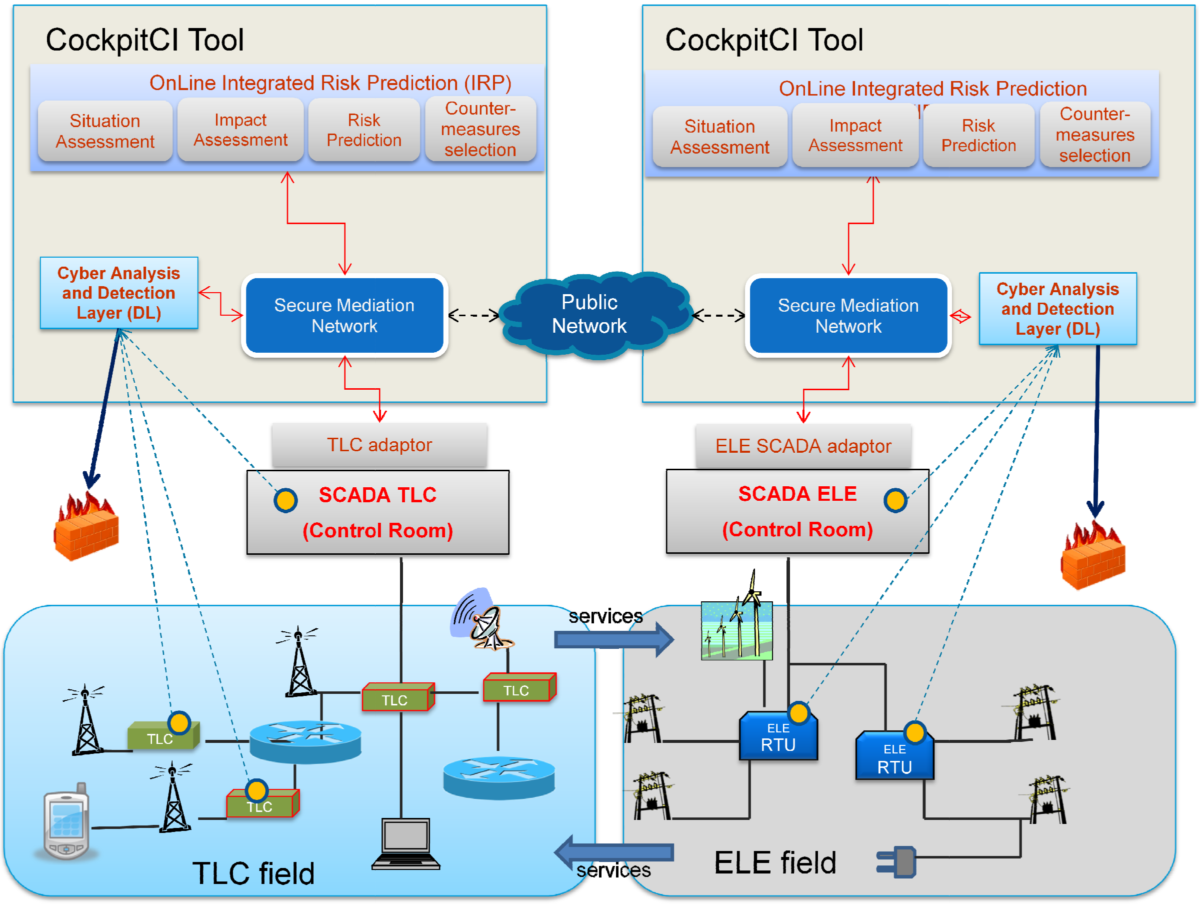


Figure 2-1 CockpitCI operational concept

Figure 2-1 shows an exemplary situation in which two interdependent CIs, an electrical CI (ELE CI) and a telecommunication CI (TLC CI), exchange services between each other, the TLC CI providing telecommunication services to the ELE CI and the ELE CI providing electric power to the TLC CI. The figure shows the SCADA control rooms, one for each CI, and the CockpitCI tool, one for each CI. The CockpitCI tools collects data from the field and the SCADA, via cyber sensing probes and the SCADA adaptor. The figure also shows the two other main components of the CockpitCI tool, i.e. the Cyber Analysis and Detection Layer (DL) which performs cyber sensing and provides cyber detection capability and the Integrated Prediction Tool (IRP) which provides situation awareness and risk assessment. The DL must also be able to enforce reaction mechanisms in response to ongoing threats, for instance through reconfiguration of a firewall (as shown in the figure). In order to provide CI Operators with a better situation awareness over the system of systems in the presence of adverse events and therefore increase the CI level of service, the two infrastructures share information via the CockpitCI tool and more specifically via the Secure Mediation Network (SMN), which provides a secure information exchange via the public network. It is important to note that the Secure Mediation Network is the only mean by which all CockpitCI system internal components can communicate with also remote corresponding modules. However, as it will be explained in section 4, the SMN plays a key-role in protecting the CockpitCI itself against possible cyber threats. The CockpitCI tool extracts two main kind of information from the underlying CI: the first one is related to the operative status of the infrastructure (e.g. commands sent to RTUs, alarms and event logs reported by the RTUs, operative status checks, etc.), and is obtained via the SCADA Adaptor (acting at SCADA Control Centre level); the second one consists of cyber information acquired via the DL probes (field adapters are deployed, when needed, to adapt all the local devices which may be source of relevant cyber-information).

The internal structure, architecture and deployment of each main component will be investigated in other project documents: the Cyber Analysis and Detection layer architecture is analysed in D3.1.1; the SCADA adaptor and IRP tool requirements, architecture and functionalities have been analysed in deliverable D4.1 - "Online Integrated Risk Predictor and SCADA Adaptor Requirements and Design" [6]; the design of the Secure Mediation Network will be performed in deliverable D5.3 –"Secure Mediation network design and specification".

The design of the CockpitCI system architecture has to take into consideration the requirements of the CockpitCI system defined in deliverable D5.1 – "CockpitCI System requirements"[1]. In [1] it is highlighted that in order to have a scalable and CI-technology independent solution (UR_11 and NFR_5), the CockpitCI tool must foresee modules acting as interface between the CockpitCI system and the specific Critical Infrastructure. Moreover, as already defined in deliverable D3.1.1 –"Requirements and Reference Architecture of the Analysis and Detection Layer-Preliminary" [2] the CockpitCI system will contain specific components enabling the detection of attack-in-progress situations such as Local Detection Agents, in charge of analysing the behaviour of CI field elements and CI SCADA system in order to propagate (both locally and remotely) information about potential critical situations. This communication flow will reach the Secure Mediation Network by means of specific Field Adaptors. The Secure Mediation Network is the component enabling all communication exchange between CockpitCI system internal components and between different CIs. It is a communication engine able to securely exchange data across public and local networks.

The Secure Mediation Network must also be able to pull/push data from/to the local IRP tool providing updated information both to local and remote peer IRP tools. Moreover, the Secure Mediation Network must provide an interface towards the Cyber Analysis and Detection Layer in order to (i) exchange cyber-attacks information with peer modules deployed in other interdependent CIs and (ii) forward cyber-attacks alarms to the Security staff of the local CI.

3 CockpitCI system architecture

In the following the system architecture of the CockpitCI tool is described in terms of information flows, functional diagrams, system configurations and operations.

3.1 Information flows

The main information flows among CockpitCI logical system components are shown in the following Figure 3-1, where the Critical Infrastructure is also shown for clarity. The DL has been split into its two constituents, the Distributed Monitoring System (DMS) which collects cyber information in the different zones in which the CI infrastructure has been segmented and the Perimeter Intrusion Detection System (PIDS), which must be able to aggregate the filtered and analyzed information of potential cyber attacks. In this figure the SMN and the adaptors are not shown since the emphasis is on logical information flows.

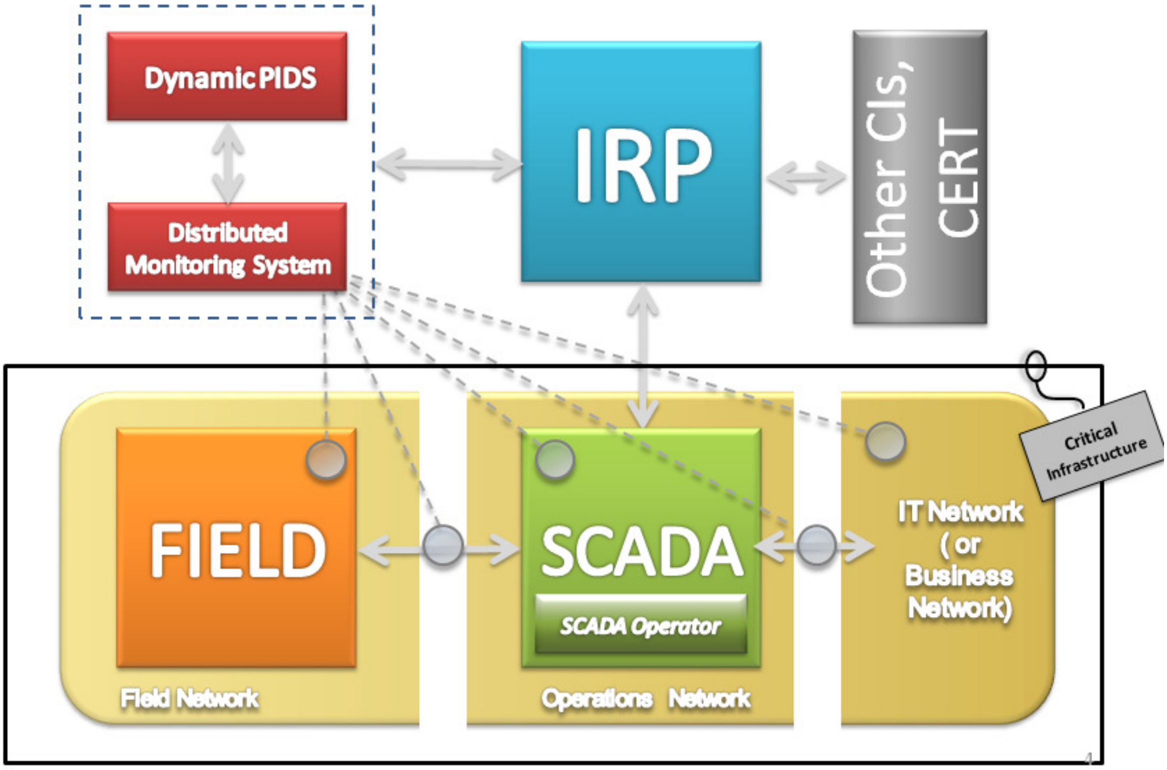


Figure 3-1: CockpitCI system logical information flows

Figure 3-2 shows the CockpitCI information flows in more detail. The input of the DL is provided by its passive sensing capability and collected all across the multi-zone system; the DL provides as an output the cyber detection parameters, i.e. the list of security events, alerts, anomalies and potential attacks occurring in the system. The IRP input consists mainly of cyber detection parameters from the DL and service parameters from the SCADA Control centre and from adjacent interdependent critical infrastructures. The IRP performs a significant task in combining cyber and SCADA information in order to assess the current situation and predict its near term evolution. The predicted service parameters are provided to the SCADA Operator and the predicted cyber parameters are provided to the Security Operator. The IRP also provides reaction strategies, i.e. recommendations to the Operators regarding the decision which should be taken and, in critical situations, also automatic countermeasures which generally will consist of cyber countermeasures.

The figure also highlights the presence of two distinct teams with different goals (the SCADA operator which is in charge of operating the CI and the Security operator which is in charge of cyber security and responsible to prevent cyber attacks). According to end-users questionnaires [1], the CI operator should receive as minimum as possible information about cyber attacks in order not to be distracted from his main duty and this information should be displayed to him in terms of possible risks to operate the CI without degradation of the SLA. On the other 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. The correct interaction among the two teams will be further specified in the course of this document.

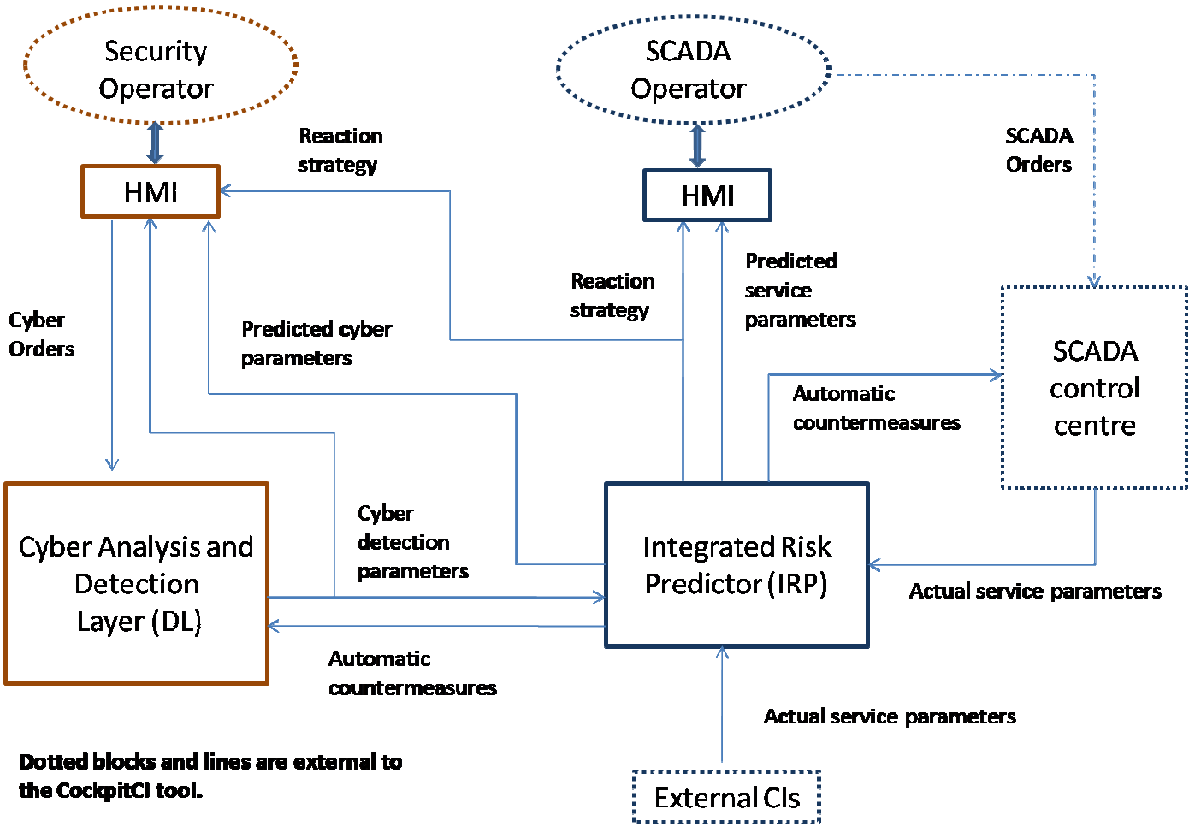

Security Operator
SCADA Operator
Reaction strategy
SCADA Orders
HMI
HMI
Cyber Orders
Predicted cyber parameters
Reaction strategy
Predicted service parameters
Automatic countermeasures
SCADA control centre
Cyber Analysis and Detection Layer (DL)
Cyber detection parameters
Integrated Risk Predictor (IRP)
Actual service parameters
Automatic countermeasures
Actual service parameters
External CIs
Dotted blocks and lines are external to the CockpitCI tool.

Figure 3-2: CockpitCI information flows

A brief description of the information flows is described below:

- **Cyber detection parameters**: information relative to potential cyber attacks; it includes information such as security events which represent symptoms of possible attacks, and therefore who is under attack, type of attack, phase of cyber attack, goal of cyber attack, effectiveness and severity of the attack,….

- **Predicted detection parameters**: same as above (ahead in time) plus risk attribute;

- **Actual service parameters**: information relative to the services and quality of services (QoS) currently provided by the CI;

- **Predicted service parameters**: same as above (ahead in time) plus risk attributes;

- **Reaction strategy**: strategies which are suggested by the IRP to Operators (they may be distinct for the two Operators) to contrast the attack (it may be a cyber attack or any other type of fault);

- **SCADA Orders**: SCADA operators may agree with the suggested reaction strategies and issue consequent orders towards (or via) the SCADA;

- **Cyber Orders**: Security Operators may agree with the suggested reaction strategies and issue consequent orders towards the Detection Layer;

- **Automatic CounterMeasures**: these are the predefined reactions which may be triggered automatically by the IRP (Operators are informed but the reaction is automatic);

These information flows will be further detailed as the work in Task 3001 and Task 4001 progresses.

3.2 Functional diagrams

The functional diagram of CockpitCI is shown in the following figures. Figure 3-3 represent an input-output view of the CockpitCI system (dotted line) whose purpose is to examine and illustrate how the system works. Within the perimeter traced by the dotted line its main functional blocks are depicted.

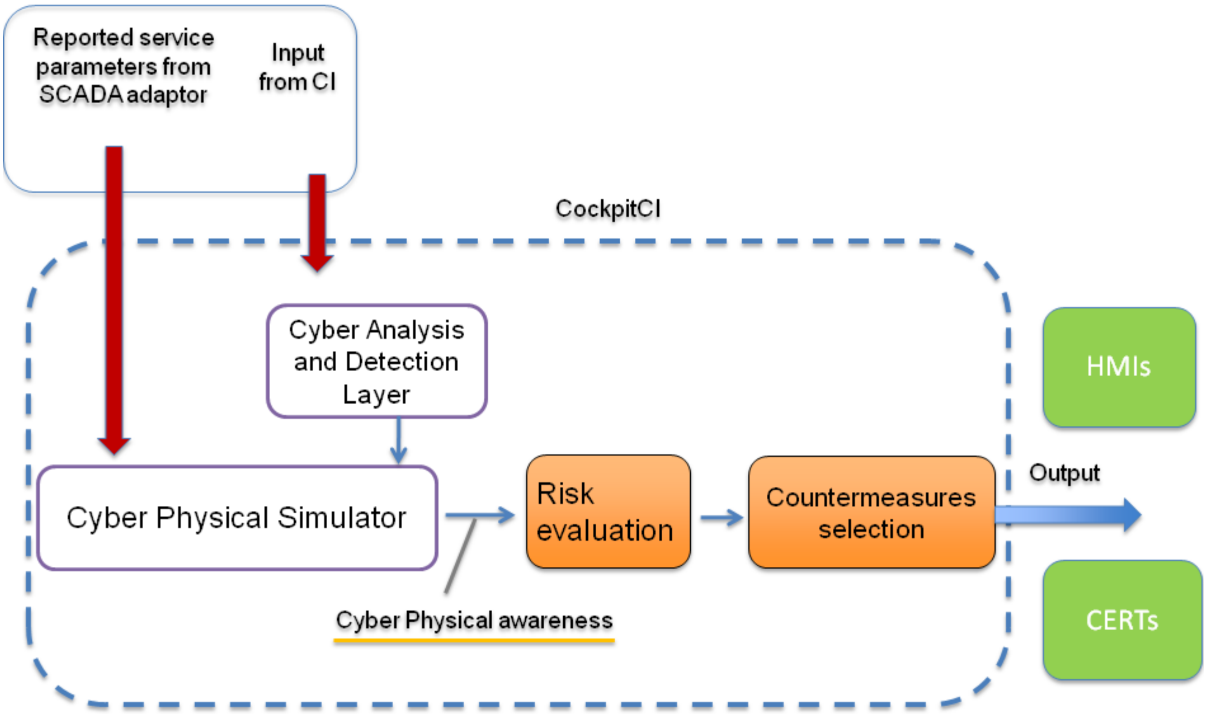

Reported service parameters from SCADA adaptor
Input from CI
CockpitCI
Cyber Analysis and Detection Layer
Cyber Physical Simulator
Risk evaluation
Countermeasures selection
Cyber Physical awareness
HMIs
Output
CERTs

Figure 3-3 CockpitCI basic functional diagram

In the input-output view two distinct input data feed the CockpitCI tool:

- Input from CI: this is all the cyber data collected by the cyber detection agents;
- Reported service parameters from SCADA adaptor: information from the SCADA.

Informations relative to potential cyber attacks, security events which represent symptoms of possible attacks, and therefore who is under attack, type of attack, phase of cyber attack, goal of cyber attack, effectiveness and severity of the attack, and other information which pertains to the Cyber Awareness definition, are extracted and aggregated by the Cyber Analysis and Detection block. This processing chain, starting from the CI raw data, performs actions of:

- Cyber events detection;
- High level correlation of security events;
- Cyber risk assessment and prediction.

SCADA service parameters and cyber parameters, at this processing level, are then combined as input of the Cyber-Physical Simulator block. This module completes the situation assessment putting together cyber information and CI/SCADA information to achieve an awareness level threshold able to activate Risk evaluation and Countermeasures selection modules.

A more detailed functional diagram of the CockpitCI tool is shown in the figure below.

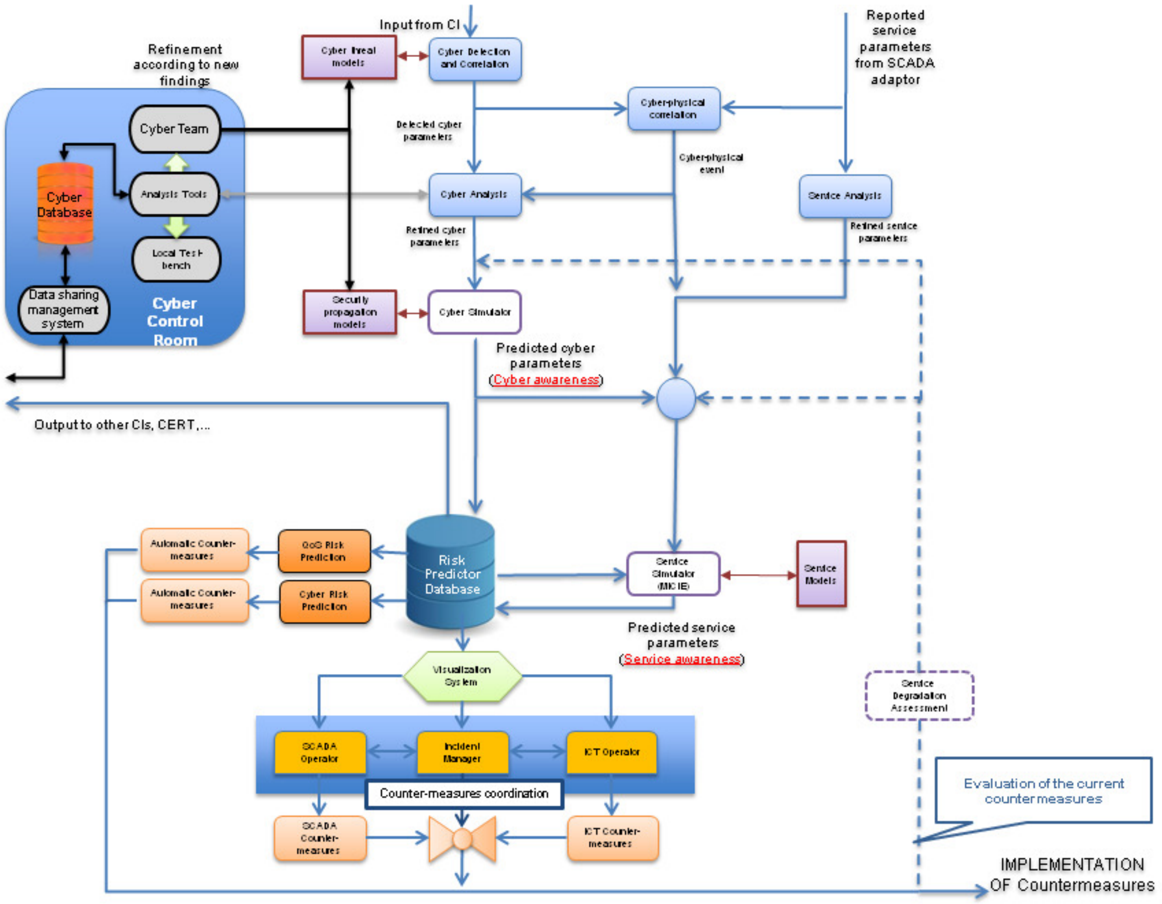

Input from CI
Refinement according to new findings
Cyber Threat models
Cyber Detection and Correlation
Reported service parameters from SCADA adaptor
Cyber-physical correlation
Detected cyber parameters
Cyber-physical event
Cyber Team
Cyber Database
Analysis Tools
Local Test-bench
Data sharing management system
Cyber Control Room
Cyber Analysis
Service Analysis
Refined cyber parameters
Refined service parameters
Security propagation models
Cyber Simulator
Predicted cyber parameters
(Cyber awareness)
Output to other CIs, CERT,...
Automatic Counter-measures
QoS Risk Prediction
Automatic Counter-measures
Cyber Risk Prediction
Risk Predictor Database
Service Simulator (MICIE)
Service Models
Predicted service parameters
(Service awareness)
Visualization System
Service Degradation Assessment
SCADA Operator
Incident Manager
ICT Operator
Counter-measures coordination
SCADA Counter-measures
ICT Counter-measures
Evaluation of the current countermeasures
IMPLEMENTATION OF Countermeasures

Figure 3-4 CockpitCI functional diagram

In the following a description of the main blocks shown in the picture will be provided. The Cyber Detection and Correlation block receives in input all the information sensed from the various zones of the CI infrastructure (“input from CI”) and performs cyber detection and correlation, i.e. it detects security events and then tries to aggregate them in security events at a higher level of abstraction. The Cyber Threat Models represents the knowledge needed to detect and correlate cyber events: it may include signatures, but also patterns of normal/abnormal behaviour related to traffic or user,..... The Cyber Physical Correlation block correlates cyber security events with information coming from the SCADA via the SCADA adaptor. This block is able to fuse data and information coming from heterogeneous fields, such as the SCADA and the electric field, in order to assess the possible underlying cyber-physical event. This is shown in the Figure 3-5 below where evidences are connected to possible causes and the network of connections may allow to infer the proper cause originating the sensed events.

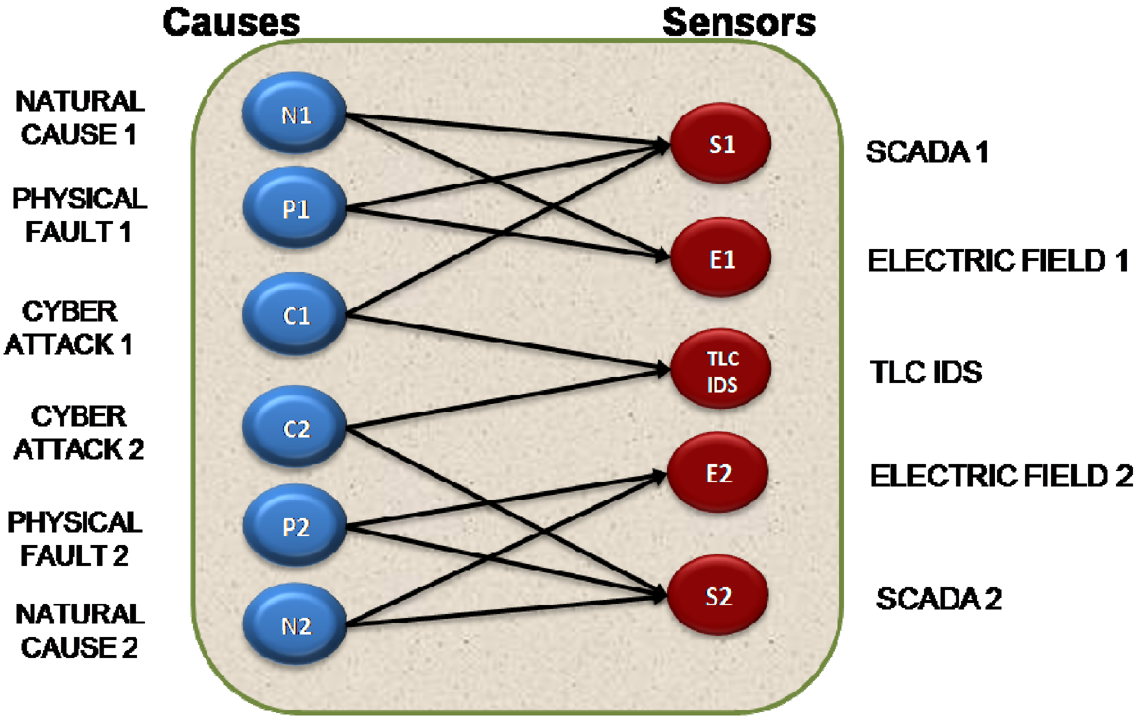


Figure 3-5 Cyber-physical correlation

The Cyber Analysis block translates the cyber parameters into refined cyber parameters. According to penetration testers, which often track malware and do a reverse job to try and understand what kind of threat it is, the Cyber Analysis is not a very easy work and often takes lot of time (as in the case of the Stuxnet analysis). The Cyber Analysis Block should be considered as a first and often rough analysis of the cyber state of the system. This block will provide an on-line analysis but will be supported and improved by off-line more accurate analysis performed by the Cyber Control Room. The Cyber Control Room is external to the CockpitCI tool. Even if some cyber-analysis can be automated and can allow to update the refined cyber parameters (especially at DL or most probably at IRP level), new threats inducing some minor incident or alarms will be deeply analysed and tested on test bench in an off-line process to refine cyber parameters and may be the cyber-model. This step is very important to ensure the sustainability of the CockpitCI system. In that aim, each local cyber control room (ideally one by CI's) will enrich its own cyber database (including malware data base, specific vulnerability of system) according to these analysis and could share this data with other cyber awareness cells and CERTs thanks to the Secure Mediation Network and according to its own sharing policy. An example of how it might work is the following:

- an abnormal network activity is detected by the Cyber Detection and Correlation block;
- the system provides these parameters (may be a sample of abnormal message) to the Cyber Analysis block;
- the Cyber Analysis block analyses the parameters but it is not able to detect anything relevant;

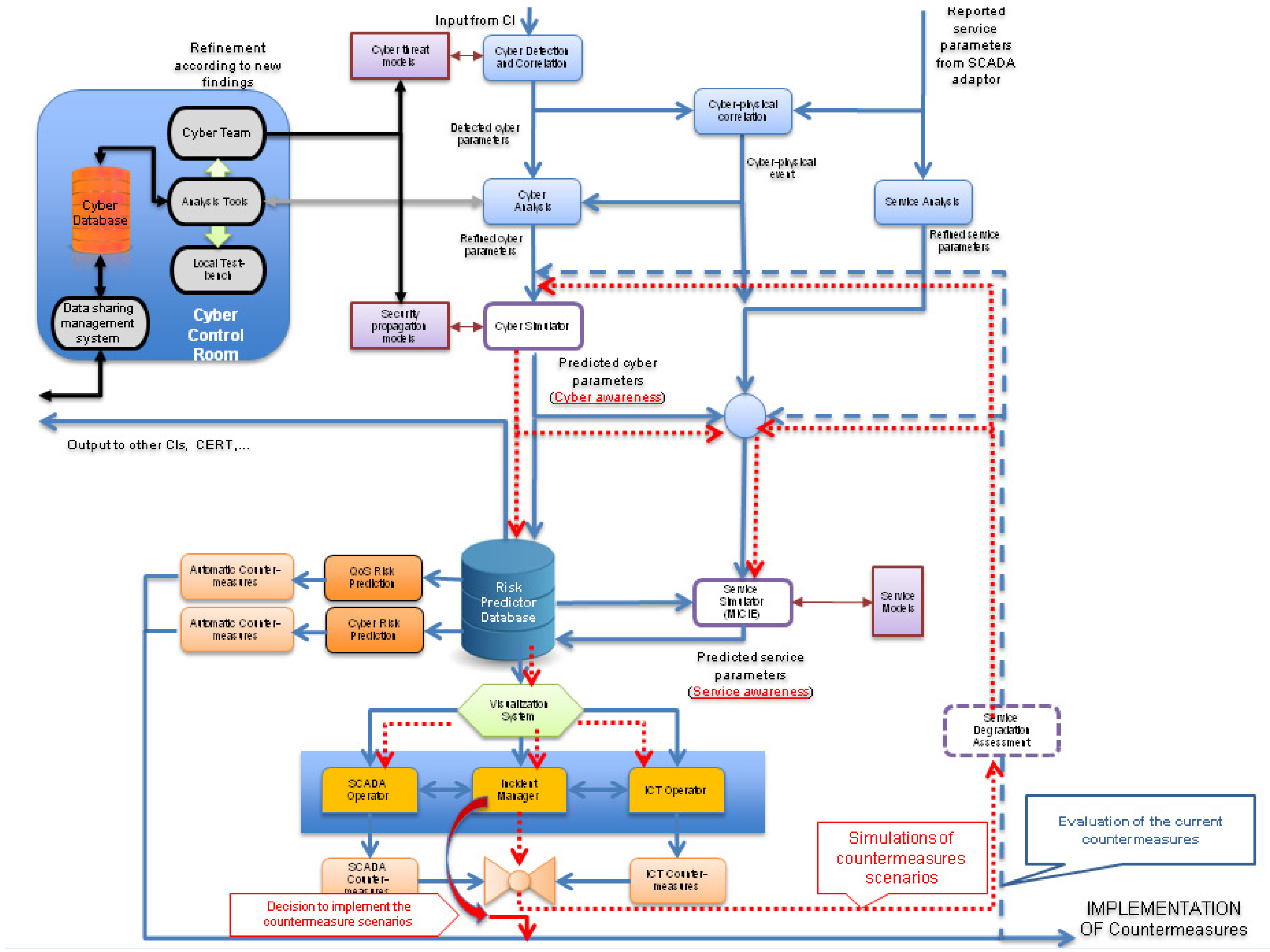
- the information (parameters, sample) could be sent to the Cyber Control Room for a deeper investigation regarding the abnormal activity;
- this dedicated analysis which can take time could lead to the discovery of a new vulnerability and a new threat and also lead to refine both the cyber-models and the cyber-analysis system layer.

The Cyber simulator is in charge of propagating the cyber threat by taking into account the probability that the infection spreads to other nodes in the network and also the topology of the network and the characteristics of the other nodes in the network. The result of this processing should lead towards a level of Cyber Awareness, where the cyber attacks currently active are recognized and their evolution in time is also assessed.

The Service Analysis block on the right processes the incoming information from the SCADA adaptor and translates it into operative levels of the elements. For example the information that the cabinet door hosting one of the RTUs is open, may result in a reduction of the operative level of the RTU itself due to physical access. The information coming from the Cyber Simulator, the Cyber-physical Correlation and the Service Analysis block is processed in the Service Simulator, which contains interdependency models and provides a picture of the CI in terms of services, i.e. which services are available and with which operative level, in the short, medium and long term.

The main objective of the CockpitCI tool is to provide actionable information to the Operators. Therefore we should imagine that two different yet coherent pictures are provided to the SCADA and the ICT Operators. The two views should reflect the knowledge and the responsibility of each Operator and a bridge between the two views should also be provided to ease interoperability and coordination. The Incident Manager is also shown in the Functional diagram as a possible approach to handle the collaboration issues at the Operator level. The first role of the incident manager is to provide during an incident the communication between the SCADA operators and ICT operators to decide the best strategy to mitigate the threat. After that the incident manager will constitute the coordination level for countermeasure to ordinate the countermeasures between the two poles of incident responses (SCADA and ICT). The simulator according to Service degradation assessment can also provide an updated picture which takes into account the effect of the current countermeasures.

An alternative scheme, though more complex, is to disconnect the feedback loop which links the decided countermeasures with the service degradation assessment system to the real application of the countermeasure, as shown in the following figure. In this case the decision to implement the countermeasure will be decided by the Incident Manager after using the CockpitCI as simulation tool to choose the better strategy.



Input from CI
Reported service parameters from SCADA adaptor
Refinement according to new findings
Cyber threat models
Cyber Detection and Correlation
Cyber-physical correlation
Cyber Team
Analysis Tools
Local Test-bench
Cyber Database
Data sharing management system
Cyber Control Room
Detected cyber parameters
Cyber-physical event
Cyber Analysis
Service Analysis
Refined cyber parameters
Refined service parameters
Security propagation models
Cyber Simulator
Predicted cyber parameters (Cyber awareness)
Output to other CIs, CERT,...
Automatic Counter-measures
Automatic Counter-measures
QoS Risk Prediction
Cyber Risk Prediction
Risk Predictor Database
Service Simulator (MICIE)
Service Models
Predicted service parameters (Service awareness)
Visualization System
Service Degradation Assessment
SCADA Operator
Incident Manager
ICT Operator
Evaluation of the current countermeasures
Simulations of countermeasures scenarios
SCADA Counter-measures
ICT Counter-measures
Decision to implement the countermeasure scenarios
IMPLEMENTATION OF Countermeasures

Figure 3-6 CockpitCI functional diagram (with simulation loop)

3.3 System Components

3.3.1 Risk Predictor operations

The functionalities of the Risk Predictor have been addressed extensively in the previous paragraph, therefore the Risk Predictor will not be further detailed.

3.3.2 Secure Mediation Network operations

The following Figure 3-7 highlights the role of the SMN as the physical means by which all information is exchanged within the CockpitCI tool. The figure also highlights the need for the SMN to provide a secure information exchange with its counterparts in the external CIs.

The figure below shows one possible architecture of the CockpitCI tool, where the SMN is depicted in the middle of the figure and is acting as communication exchange facilities for all the elements of the system, and also providing communication services between the Distributed Monitoring Systems and the Dynamic PIDS.

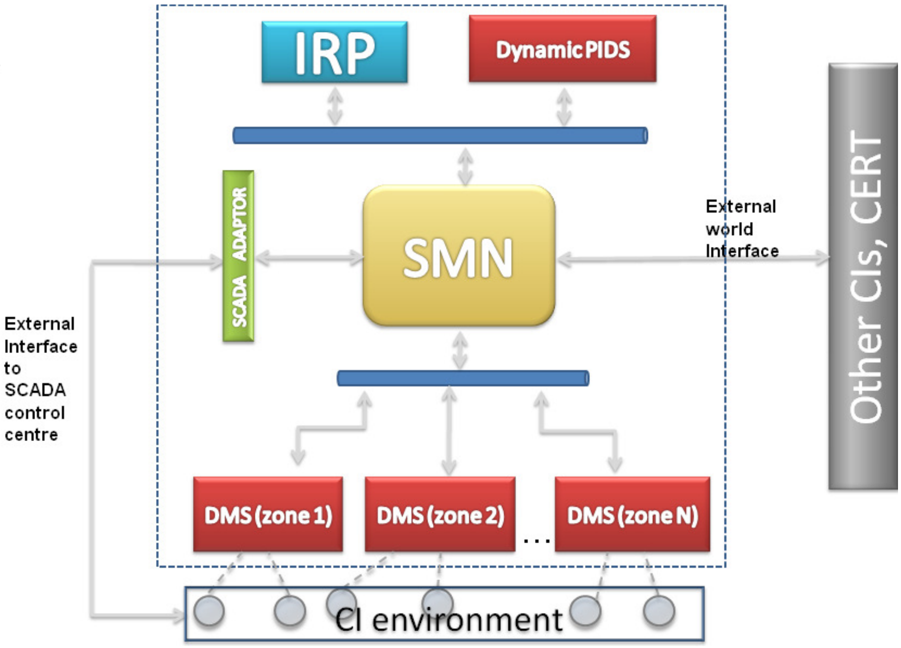


Figure 3-7 CockpitCI possible scheme

However the communication among distributed IDS may be accomplished effectively by a standard family of protocols (i.e. IDMEF, BEEP,etc), which have been developed specifically with this purpose in mind and enable the transfer and normalization of event data necessary for cross platform capture and analysis of intrusion detection data [3]. Therefore the following scheme shown in Figure 3-8 is proposed which highlights the interfaces with the external world and also the internal interfaces among CockpitCI components.

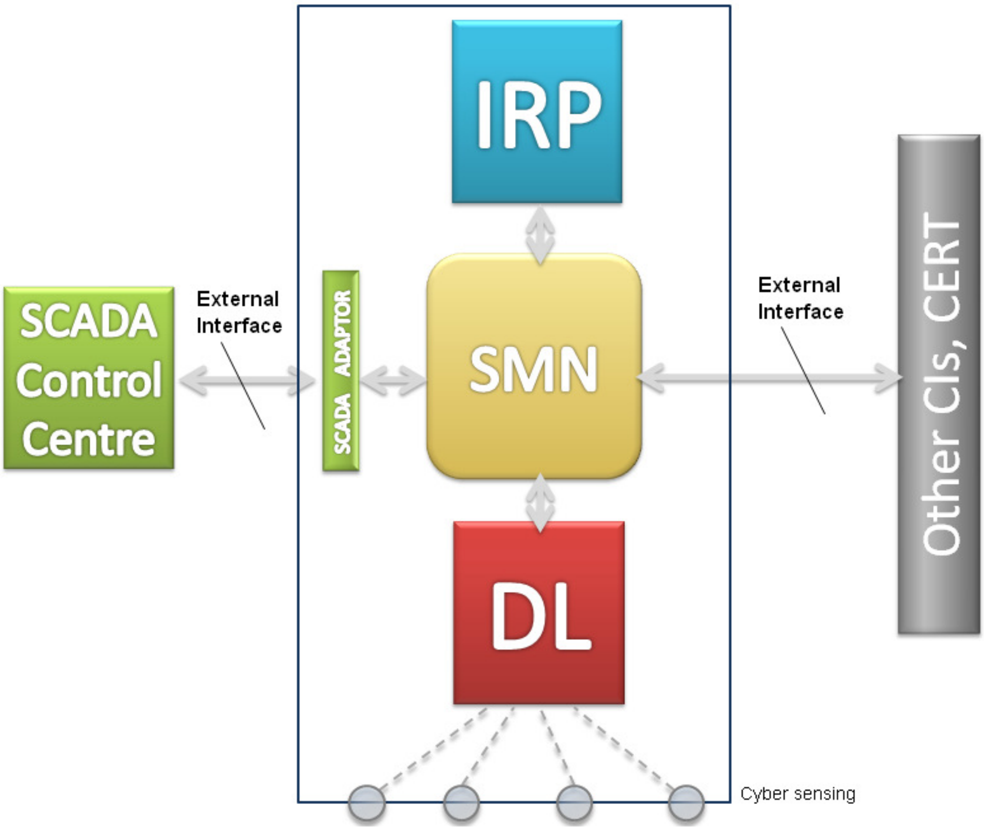


Figure 3-8 CockpitCI interfaces, final scheme

3.3.3 Cyber Analysis and Detection Layer operations

The purpose of this section, after a short and general introduction, is to review some of the concepts and mechanisms introduced in this layer [2] in order to better understand their impact on the overall architecture.

Control Systems (e.g. SCADA systems) are used to automate common processes. These systems need to provide reliable and safe automation for such critical infrastructures such as power grids and telecommunication networks. The critical necessities for both government and its people to survive are automated using industrial control systems. In the past decade, advances in technology have added automation that has intertwined of these systems with the Internet, wireless, business networks and traditional hardware and communications protocols. Many Control Systems (CSs) are in some way electronically connected to networks of less trust, potentially even a slight distance away from the Internet. These CSs typically use vulnerable communication protocols. Many even use TCP/IP and in specific situations, common off-the-shelf hardware and chipsets. It is paramount to the safety of our society to sufficiently understand the architecture of and protect these critical systems. Thus, the paradox is that CIs massively rely on the newest interconnected and vulnerable, Information and Communication Technology (ICT), whilst the control equipment, legacy software/hardware, is typically old. Such a combination of factors may lead to very dangerous situations, exposing systems to a wide variety of attacks. To overcome such threats, the CockpitCI produce advance intrusion detection, analysis and reaction tools to provide intelligence to field equipment.

SCADA systems have always been susceptible to cyber-attacks. Different types of cyber-attacks could occur depending on the architecture and configurations used in the SCADA system. These attacks fall into one of the following four categories:

1. Internal/Non-malicious - employees or contractors causing unintentional damage;

2. Internal/Malicious - system users with extensive internal knowledge of the system who intentionally cause damage;

3. External/Opportunistic - hackers seeking a challenge;

4. External/Deliberate - malicious, well-funded political activists, organized crime groups, or nation states.

All classifications of attacks can result in serious consequences. To protect cyber infrastructure from the above attacks, a growing collaborative effort between cyber security professionals and researchers from private and academia has involved in designing a variety of intelligent cyber defence systems.

Cyber defence systems monitor the activities that occur in a computing resource to detect violations of a security policy of an organization. These violations may be caused by people external to the organisation (i.e. attackers) or by employees/contractors of the organisation (i.e. insiders). During the recent past, cyber detection has received considerable motivation owing to the following reasons:

1. If a cyber-attack is detected quickly enough, an intruder can be identified quickly and ejected from the system before any damage is done or any data are compromised. Even if the detection is not sufficiently timely to pre-empt the intruder, the sooner that the intrusion is detected, the less is the amount of damage done and the more quickly that recovery can be achieved.

2. An effective cyber defence system can serve as a deterrent, acting to prevent cyber-attacks.

3. Cyber-attack detection and analysis enables the collection of information about intrusion techniques that can be used to analyse the new threats and to strengthen the intrusion prevention facility.

Along with the above motivations, the intention of the cyber defence system can be summarised as follows:

1. Detect as many types of attacks as possible (i.e. including internal malicious/non-malicious and external opportunistic/ deliberate attacks), thereby increasing the detection rate;

2. Detect and analyse attacks as accurately as possible, thereby reducing the number of false alarms;

3. Detect and analyse attacks in the shortest possible time, thereby reducing the damage of the attacks.

The above requirements have prompted researchers to develop cyber defence systems that fulfil the above goals to prevent SCADA systems from cyber-attacks.

The Cyber Analysis and Detection layer provides cyber detection and analysis capability, but also reaction capabilities. The architecture originates from the following process:

- reuse cyber architecture concepts (e.g. segmentation, multilevel correlation, ...) which are commonly adopted in the IT world and also adopt its well established security solutions (e.g. NIDS, HIDS, honey-pots,...);
- adapt and evolve these concepts and solutions in order to take advantage of specific features of SCADA systems (e.g. more regular traffic patterns, ...);
- introduce additional mechanism specific for the SCADA domain.

In the following a classification of the cyber mechanisms introduced in [2] in terms of their role and attack phases in which they are active, is proposed. Table 3-1 provides a classification of cyber mechanisms according to the following characteristics:

- standard IT security solution or novel security solution;
- capability to perform detection, reaction or both, with respect to a cyber threat.

	IT standard solution	**Detection**	**Reaction**	**Remarks**
NIDS, HIDS	**Yes**	✓		
IPS	**Yes**		✓	With the terms IPS generally we mean Intrusion Detection Prevention Systems. For clarity in this document we would like to consider IDS and IPS as two complementary not overlapping mechanisms. Intrusion Prevention Systems typically terminate a connection or block all traffic from a certain IP address.
Honeypot	**Yes**	✓	✓	The honeypot is able to detect a cyber intrusion but it also allows to neutralize the intruder by confining it into the honeypot enclosure.
Correlation engines	**Yes**	✓		The correlation engines allow to detect complex or distributed attacks.

BMS	**No**		✓	The Backup Master Station is able to coordinate a set of local RTUs.
Heart-Beat mechanism	**No**	✓		The heart-beat mechanism allows to detect the situation when one or more elements are isolated.
Smart RTU	**No**	✓	✓	The Smart RTU is not a component of the Cyber Analysis and Detection Layer, nor is it a topic of WP3000; yet it is convenient and reasonable to include it in this list.
Shadow RTU	**No**	✓		It detects an alteration of RTU behaviour and possibly other types of attacks.

Table 3-1: Cyber mechanisms versus detection/reaction

When it comes to cyber detection, it is also of interest to understand in which phase of the cyber attack these mechanisms are effective. A cyber attack usually comprises the following phases:

1. **reconnaissance**, in which the attacker finds out the information he needs to actually get in (e.g. what traffic the firewall lets through, what hosts are in the network, what services they actually have running, etc …);
2. **penetration**, in which the attacker gains the access he needs to achieve his goal (e.g. this might involve multiple steps, first to gain access to “another host", and then to use that access to get into the target host);
3. **exploitation**, in which the attacker performs the bad stuff that motivated his getting this illicit access (e.g. stealing data,….);
4. **conclusion**, in which the attacker takes whatever steps are necessary to cover his own tracks.

Cyber detection mechanisms may be active in one or more of the four cyber attack phases which have been identified, as shown in the following Table 3-2.

	Cyber Phase 1 Reconnaissance	**Cyber Phase 2 Penetration**	**Cyber Phase 3 Exploitation**	**Cyber Phase 4 Conclusion**
NIDS, HIDS	✓	✓	✓	✓
Honeypot	✓	✓		
Correlation engine	✓	✓	✓	✓
Heart-Beat mechanism			✓	

Smart RTU			✓	
Shadow RTU			✓	

Table 3-2: Cyber detection mechanisms versus cyber attack phase

As shown in the table, standard IT security solutions are generally able to detect a cyber attack in each cyber attack phase: of course cyber detection should be performed preferably during phase 1 or phase 2 before the attack starts to deliver its bad effects, detection in a later phase is an evident indication of failure. On the contrary the novel cyber security mechanism introduced in [2] are capable of detecting a cyber attack in phase 3. These mechanisms are in fact focused on detecting functional alterations, i.e. modifications to the normal behaviour. Smart RTUs for example will detect abnormal commands or apparently licit commands which may be disruptive in the current context. The shadow RTU will detect alterations to normal RTU behaviour. This functional based approach provides increased robustness to CockpitCI detection capability and is suited to work in tandem with reaction mechanisms which try to reduce the impact of an attack.

3.4 System architecture diagrams

It is interesting to extract some remarks which were made by the end-users regarding the scope of the system in the End-User Questionnaire, which is appended at the end of D5.1 ([1]). Regarding reaction capabilities and local intelligence, the questionnaires reports the following answers:

- “CockpitCI should be a decision support system and should not be connected to any CI equipment”.
- “CockpitCI tool shall be configurable to a passive mode where attacks and suspicious traffic is detected and reported, but no active actions are taken.”
- “…….the CockpitCI tool shall have the possibility to automatically start a reaction 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";
- “….the system must pass very strict testing and QA procedures….”;
- “…..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”;
- “…..in some extraordinary situations 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”;

The answers provided by End Users are basically conservative, yet they are also open to investigate unconventional approaches. Therefore two different version of the CockpitCI architecture are investigated, a basic version and an advanced version which intends to investigate and experiment automatic reaction capabilities. The two tool versions have been derived taking into account the constraints that for SCADA legacy system no change to the existing configuration can be accomodated.

More precisely for legacy SCADA system the CockpitCI tool basically provides decision support capabilities, i.e. the proposed new tool is able to provide the operator with a better situation awareness in case of critical events (Critical events, as largely described in previous deliverables, include Cyber Events) and it is completely passive. These main capabilities are fully accomplished by the basic version of the tool, therefore its acceptance by End Users should be high.

On the other hand, the automatic reaction capabilities described within the document have been introduced to fulfill the project objective of business continuity and resilience. The advanced version of the tool needs to be properly addressed, in general it will not be easily accepted easily by End Users, but reasonable compromises could be achieved. Automatic reaction which follows pre-defined courses of action seems to be acceptable by End Users.

The basic interpretation of automatic reaction is that of safe mechanisms which automatically put zones under attack into a pre-determined safe state in case of isolation from the SCADA control Centre. Therefore, they are based on automatic mechanisms which need to be directly connected with the Field zone of the Critical Infrastructure. Finally it should be noted that automatic protection mechanisms are already adopted in several situations; for example, as noted in [7], "*when major disruptions occur on a power system, the transmission network automatically responds by breaking into self-contained islands, according to fixed procedures established well in advance. Such procedures have not generally been updated since the onset of deregulation and will not be adequate for dealing with a terrorist attack on multiple carefully chosen targets. Rather, we need a more flexible islanding method that can react instantaneously to attack conditions, taking into account the location and severity of damage, load status, and available generation*". This kind of adaptive and intelligent reaction is perfectly in line with the objectives and aims of the CockpitCI project.

The following Table 3-3 tries to classify the list of cyber mechanisms proposed for the DL, in terms of:

- Passive/reactive, i.e. does the cyber mechanism introduce an automatic reaction and therefore possibly alter the operation of the SCADA ?
- does the introduction of the cyber mechanism require a change in the configuration of the SCADA system (which is not permissible in legacy SCADA systems) ?

	Passive / Reactive	**Configuration change**	**Comments**
NIDS, honeypots, correlation engines, shadow RTU	Passive	NO	They are all passive modules.

HIDS	Passive	YES	Software should be installed on legacy SCADA hardware.
BMS, IPS (including firewalls)	Active	YES	BMS may perform local coordination of a set of RTUs.

Table 3-3: Cyber mechanisms main characteristics

Cyber mechanisms in row 1 are perfect candidates for the basic architecture; mechanisms in row 2 and 3 are candidates for the advanced architecture.

3.4.1 CockpitCI system basic configurations

The leading idea is to build an additional layer, the CockpitCI tool, which cannot alter the current operation of the Critical Infrastructure and makes the Critical Infrastructure more robust to cyber attacks and faults by increasing Situation Awareness and supporting Risk assessment and Decision Making. The basic configuration of the architecture does not address automatic reaction capabilities. The basic configuration includes the cyber mechanisms listed in the first row of the Table 3-3.

It is very important in fact for Critical Infrastructures to provide minimal level of services even under active attacks or if partially compromised.

The following figure recalls the previous schematic diagrams and expands the Detection Layer in order to properly visualize its distributed nature. The Detection Layer is split into two constituents, the centralized part (PIDS) which is hosted in the SCADA Control Centre and the distributed part (DMS) which is dispersed in the different zones.

As anticipated, the figure includes only the Detection Layer mechanisms which do not alter the operations of the SCADA system and do not change the configuration of the SCADA system.

The Figure 3-9 highlights the fact that the CockpitCI tool is built on top of the Critical Infrastructure and that a distributed architecture that aggregates several probing and monitoring points works together to provide the surveillance capabilities. Multiple different zones (or networks) must be monitored and NIDS perform intra-zone and inter-zone monitoring. The shadow RTU monitors the I/O of the RTU and triggers an alert whenever it senses a mismatch or model discrepancy. The CockpitCI tool provides an interface towards SCADA Security Operators.

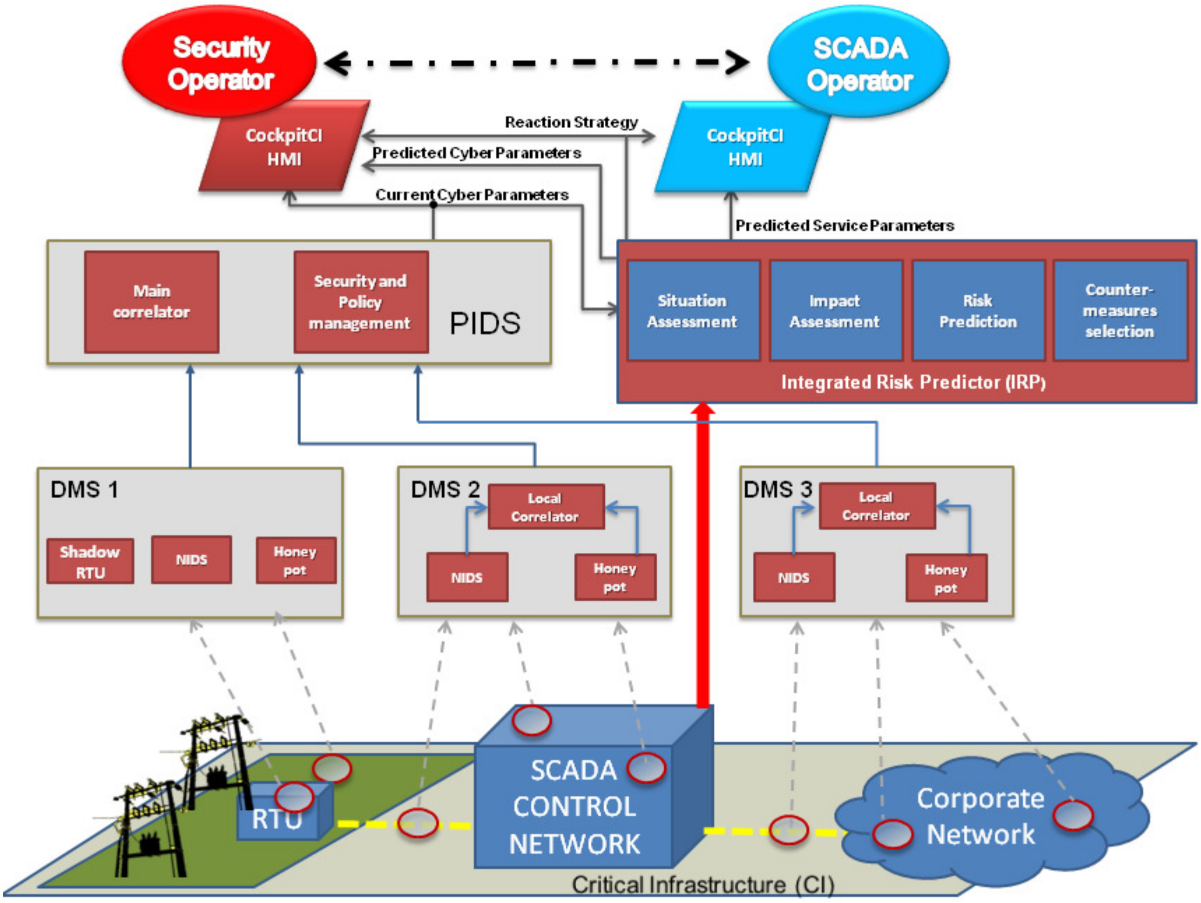


Figure 3-9 CockpitCI basic configuration

Remarkable features of the architecture are:

- the tool cannot alter or delay the functioning of the CI since the cyber sensing is passive and the tool relies (preferably) on its own communication means;
- the data is collected and analyzed and presented to the Operators to support the decision making process.
- two operator teams are at work, the SCADA operator and the security operator; the coordination, synergy and exchange of information between the two teams will be further discussed in the course of this document;
- all cyber sensing elements are supervised and controlled by the Security and Policy Management block.

3.4.2 CockpitCI system advanced configuration

The advanced configuration of the CockpitCI tool includes automatic reaction capabilities. **Automatic reaction** is one additional capability of the tool, which needs to be handled with care and which may trigger automatically and **in near real-time** mechanisms that prevent the attack from generating a full system failure.

The following Figure 3-10 shows the advanced configuration of the architecture, which now includes the Field Security Manager (the FSM hosts the BMS and heartbeat logic), Host Intrusion Detection Systems and Intrusion Prevention Systems and shows (**highlighted in yellow**) examples of the automatic reaction capability which may be triggered by the CockpitCI tool.

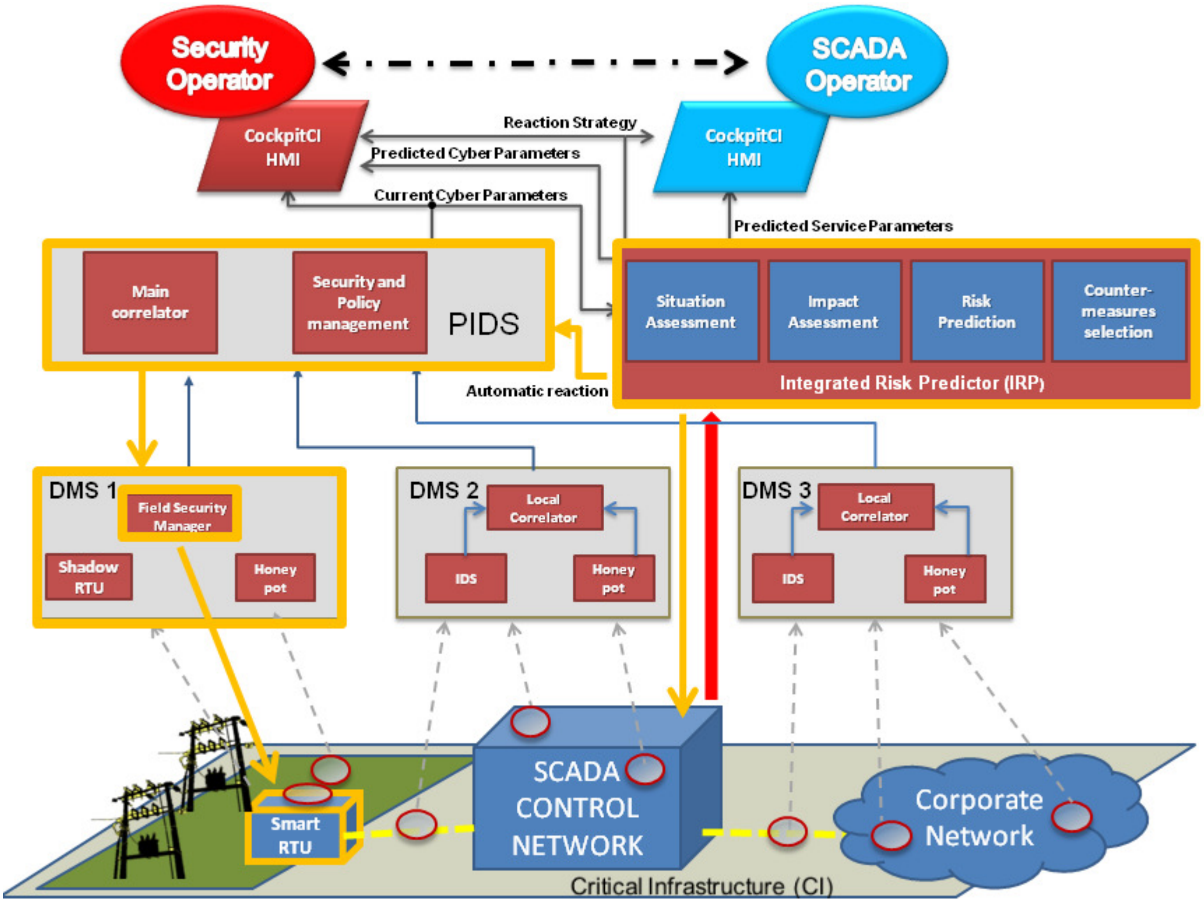


Figure 3-10 CockpitCI advanced configuration

The exemplary automatic reaction capabilities shown in the figure are:

1. The IRP triggers the system into a more conservative and defensive posture (e.g. the Security and Policy Management performs a reconfiguration of the firewall, where the firewall may be an already existing one or a new one provided with the CockpitCI tool; in this way the propagation of an attack may be blocked and portions of the network may be isolated for precaution);

2. The IRP triggers the SCADA control centre so that a predetermined safe-mode state is reached; e.g. the level of alert could be raised to a level where all SCADA components will perform additional (e.g. double) checks before executing a command;

3. Deployment of "smart RTUs", where RTUs in critical situations may refuse to execute commands (e.g. in presence of abnormal commands or licit commands which are considered malicious in the current context);

4. The Field Security Manager, in case of isolation from the SCADA control centre, may coordinate the set of local RTUs to perform pre-determined actions; pre-determined actions may be reprogramming, shutdown, switch to safe-mode state,…..………

3.5 System Operations

In the following we describe the CockpitCI operation/behaviour in presence of cyber attacks which may affect the RTUs, the SCADA control centre and the communication network. In accordance with the detection capability of the novel cyber detection mechanisms, it is assumed that the attack is already in the exploitation phase (phase 3).

The first Table 3-4 addresses the situation where the cyber attacks affect the RTUs. Columns 2 and 3 illustrate the sequence of actions occurring at the DL and the IRP in presence of the cyber attack.

	DL	IRP
RTU software or parameters are changed / corrupted.	- The Shadow-RTU detects the I/O mismatch occurring at the RTU; -The Shadow-RTU informs the DL about the mismatch; -The DL correlates this info with additional Security events/alarms; -The DL sends the cyber picture to the Security operator and to IRP.	- IRP performs situation assessment and runs the cyber and service simulator to predict future evolution of the situation from a cyber and service perspective; -IRP may suggest automatic reaction strategy to Operators or authorize the execution of automatic countermeasures.
RTU is compromised (e.g. running very slowly).	- The Shadow-RTU detects the deviation from the expected behaviour (e.g. slowdown of RTU response time); -The Shadow-RTU informs the DL about the deviation; -The DL correlates this info with additional Security	Same as above

	events/alarms; -The DL sends the cyber picture to the Security operator and to IRP.	

Table 3-4: System operations when cyber attack affects RTUs

CockpitCI operation/behaviour in presence of cyber attacks on the SCADA control centre is shown in the following Table 3-5.

	DL	IRP
SCADA control centre receives fake information, so to disguise unauthorized changes or to cause the operator to initiate inappropriate actions.	-The Shadow-RTU may perform as "message repeater" using the Shadow-RTU loop and this allows to verify that the information sent by RTU is not the same as the one arriving at SCADA; -Shadow RTU reports to the DL (Detection Layer); -DL immediately alerts the Security Operator and SCADA Operator; -DL correlates this info with additional Security events / alarms and sends the result of the elaboration to the Security operator and to IRP.	-IRP uses the DL information about cyber events to perform risk assessment and situation awareness; -IRP provides the results of this assessment to the SCADA Operator (and eventually to the Cyber Operator).
SCADA SW is intentionally compromised.	- HIDS detects the situation and reports to the DL (Detection Layer); -DL immediately alerts the Security Operator and SCADA Operator; -DL correlates this info with additional Security events / alarms and sends the result of the elaboration to the Security operator and to IRP.	Same as above.
SCADA parameters are	No detection unless the Smart RTU has enough	Same as above.

compromised.	intelligence and knowledge to recognize some kind of anomaly.	
Computer performance are compromised (e.g. virus infections slowing down all operations)	HIDS reports to the DL (Detection Layer) and Security Operator and IRP.	Same as above.

Table 3-5: System operations when cyber attack affects SCADA control centre

The following Table 3-6 describes the CockpitCI operation/behaviour in presence of cyber attack on the communication network.

	Smart RTU	DL	IRP
Communication channels are congested (e.g. DoS)	-The Smart-RTU may recognize a congested situation and notify this fact to the SCADA Control Room	- The NIDS will also detect the situation;	-IRP simulates a scenario in which the communication channel is congested and transfers the result of its analysis including possible counter-actions to the SCADA Operator and to the Security Operator.
Message flow to/from RTU-SCADA is manipulated (e.g. man in the middle attack)	-If commands are malicious or anomalous, the Smart-RTU may detect the situation; -the Smart-RTU may then discard commands and send an alert to the SCADA Control Room; -Smart RTU enters in a Safe state mode.	-The Shadow-RTU may act as "message repeater" and allow the DL to recognize the situation; -The Shadow-RTU may also "catch" the alert issued by the smart RTU and "repeat" it along the separate CockpitCI communication network (in this way it would not be intercepted and neutralized by the	

		MITM attack);	
RTU is isolated from the SCADA (e.g. DoS attack).		-Via the Heart-Beat mechanism, and/or via NIDS (detecting huge volume of data traffic on the RTU-SCDA link), DL recognizes that the RTU is isolated from the SCADA; -BMS starts to coordinate the RTU; -BMS sends an alarm to the SCADA Operator and to the IRP.	- IRP simulates a scenario in which the RTU is isolated and transfers the result of its analysis including possible counter-actions to the SCADA Operator.

Table 3-6: System operations when cyber attack affects communication network

4 System interfaces

4.1 Identification of system interfaces

This section is devoted to the identification and the description of system interfaces existing among the CockpitCI tool main components (as defined in Section 3) and the interfaces arising between the CockpitCI tool (i.e., its various modules) and the external environment (e.g. interfaces towards interdependent CIs, public networks, authorities, CERTs, etc.). Since the CockpitCI tool is a proper extension of the MICIE tool, the work of interfaces definition will be done by leveraging past knowledge and results from MICIE project [4].

The task of interfaces definition starts with the fundamental distinction between *external* and *internal* interfaces. We call *external interfaces* those interfaces arising between modules of the CockpitCI tool and external entities (belonging or not to the CI where the considered CockpitCI tool is installed). Reasoning in the same way, we call *internal interfaces* the interfaces existing between two or more components of the same CockpitCI tool. We can further distinguish between external interfaces involving the CockpitCI tool and an entity belonging to the same CI (we call them *external intra-CI interfaces*) and external interfaces between the CockpitCI tool and an entity which does not belong to the same CI (*external inter-CI interfaces*). Thus, the adjectives external/internal here refer to the CockpitCI tool, not to the underlying CI.

Figure 4-1 displays the main functional blocks composing the CockpitCI tool, as well as the main internal and external interfaces involving the CockpitCI tool and the underlying CI.

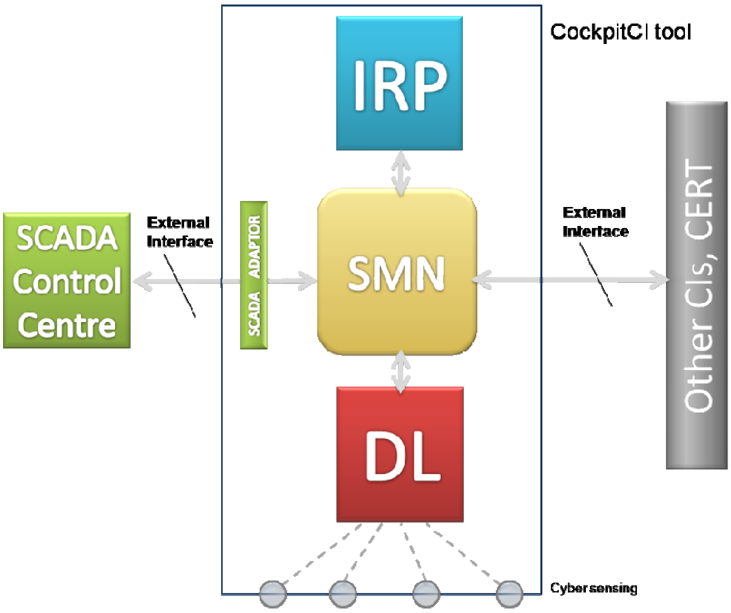


Figure 4-1 CockpitCI system physical interfaces

It should be noted that internal interfaces between CockpitCI modules could be seen from two different perspectives, namely (i) *logical interfaces* (i.e. interfaces that ideally link two CockpitCI system modules, for example when one module uses data coming from another one) and (ii) *physical interfaces* (i.e. the interfaces physically enabling the above mentioned logical information flows). We refer to the physical system interfaces, i.e. to the actual physical scheme of the logical relations between systems and actors, as defined by the CockpitCI approach. It is worth noting that, while the logic architecture directly derives from the CockpitCI approach, different deployments in terms of physical architecture are possible (different choices are possible, in relation to the type of CI, the desired performances of the resulting system, the available budget, etc.). Also, internal interfaces are "standard interfaces" (i.e. defined univocally by CockpitCI framework); instead, the realization of the external interfaces may depend in general on the specific CI technological constraints.

The following subsections present a list and a description of external and internal system interfaces, in terms of main functionalities supported, flow of information between the actors involved (message sequence chart diagrams) and description of the messages exchanged (detail of message parameters). Interfaces can be easily identified and described starting from the analysis of the physical CockpitCI architecture. In particular, the reader is referred to Figure 4-2, which is reported here for convenience.

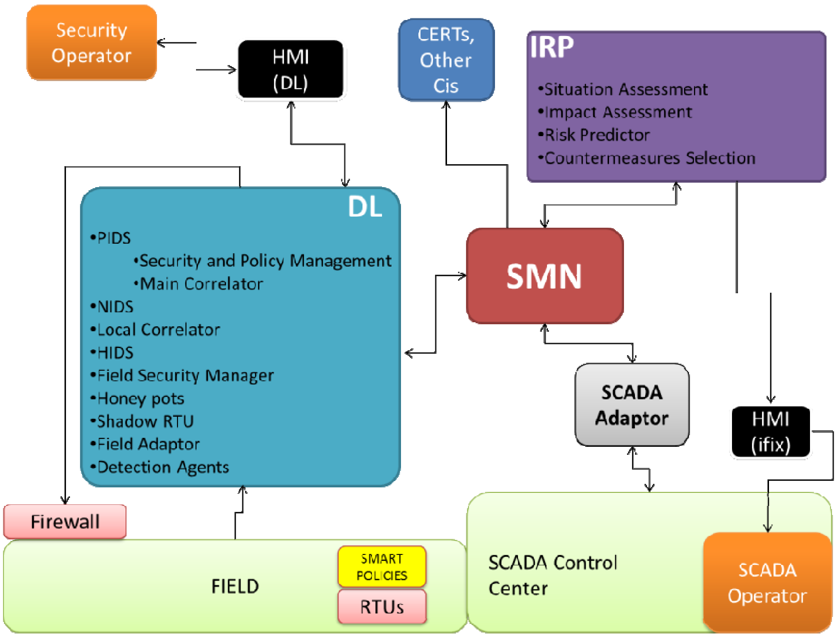


Figure 4-2: Physical interconnection between the CockpitCI main components and the underlying CI.

A the centre of the CockpitCI tool physical architecture is the Secure Mediation Network, which mediates the flow of information among the Detection Layer, the Integrated Risk Predictor and the SCADA Adaptor. These are the main functional blocks of the CockpitCI tool. All the interfaces at this central level of the architecture are bidirectional, allowing also to put in place a feedback of enriched information from the tool (mainly from the IRP and the DL) to the CI field, as it has been described in details in the previous sections.

Connections with the underlying CI are represented in the bottom of the figure. The DL catches information from the Field in a transparent way. Information is adapted, processed and transmitted to the SMN and to a HMI, which enables interaction with the Security Operator. The Security HMI allows the Security Operator to implement cyber-reaction strategies. The architecture also permits the DL to autonomously implement cyber-reaction acting, e.g., on firewall settings. A second HMI connects the SCADA Operator with the IRP, allowing visualization of relevant information related to e.g. the predicted services operative level. Based on this information, the SCADA Operator may decide to put in place countermeasure (which may also be suggested by the IRP) by sending commands to the field via the SCADA Control Centre. Finally, the interface between the block "CERTs and other CIs" and the SMN allows mediation of information between linked CIs and other relevant sources of information (e-g- CERTs), allowing to raise awareness in a more complete and integrated way.

4.2 External Interfaces

To correctly perform their functionalities, the CockpitCI system modules need to exchange information (e.g. data, measurements, status notifications, alarms, commands, etc.) with a number of components, systems and actors belonging to the underlying CI. Referring to the system architecture description given in Section 3, it is possible to identify the following fundamental *external* and *intra-CI* interfaces (refer to Figure 4-1 and Figure 4-2):

1) ***SCADA Adaptor – SCADA Control Center i/f:*** the interface enables exchange of information between the SCADA Control Center and the CockpitCI system, via a properly designed SCADA Adaptor.
2) ***Detection Layer – CI Field i/f:*** interface between the CockpitCI Detection Layer and the zones of the underlying CI (e.g. interfaces involving detection agents, shadow RTUs, honeypots, etc.).
3) ***Security Operator Human-Machine i/f (HMI):*** interface enabling interaction between the CI Security Operator and the CockpitCI Detection Layer (visualization of predicted cyber parameters, suggested cyber reaction strategies, transmission of cyber orders to the Detection Layer, etc.).
4) ***SCADA Operator Human-Machine i/f (HMI):*** interface enabling interaction between the CI SCADA Operator and the CockpitCI Integrated Risk Predictor**,** for visualization to the SCADA Operator of IRP knowledge regarding the operative status of the CI, including predicted service parameters and suggested reaction strategies.
5) ***Secure Mediation Network – Operator control i/f***: control interface between the CockpitCI Secure Mediation Network and a human Operator. It is used for configuration, management and status checking of the CockpitCI tool functionalities from the SMN point of view.

Basically, external intra-CI interfaces are related to the needs of (i) data acquisition from the field and communication of the IRP knowledge back to the field and the Operators and (ii) enabling communication between Detection Layer internal components with CI's field components (e.g. firewalls reprogramming).

Interdependence between linked CIs and, more in general, with the external environment must be considered in order to get a fine situation and CI status assessment. Therefore, the CockpitCI architecture must consider also external interfaces towards all the relevant actors outside the CI in question, including:

6) ***Secure Mediation Network – Secure Mediation Network i/f***: interface between Secure Mediation Networks belonging to different linked CIs (e.g. interface between the Secure Mediation Network of the CI in question and a public network).

In the following, a detailed description of each of the aforementioned external interfaces will be provided, including message sequence chart diagrams (showing the flow of information between actors involved) and specific message description in relation to relevant functionalities to be considered.

4.2.1 SCADA Adaptor – SCADA Control Center interface

The interface between the SCADA infrastructure and the CockpitCI tool enables two way communication and exchange of information between CI's appliances and the CockpitCI system. SCADA adaptors are the abstraction layer between SCADA appliances and the Secure Mediation Gateway. For the sake of completeness here is reported the Figure 4-3 that describes SCADA Adaptor's architecture, also provided in deliverable D4.1.1.

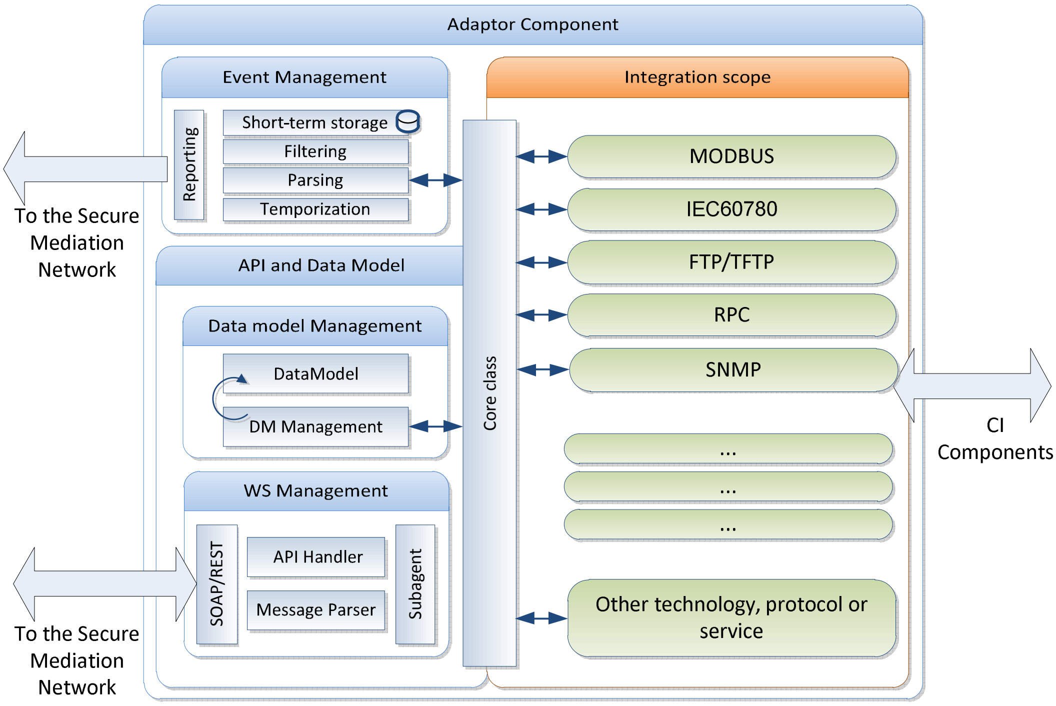


Figure 4-3: SCADA adaptor architecture

The interface described here (SCADA Adaptor-SCADA System) is on the right side of the picture. Abstraction is achieved by means of a suitable Data Model of the underlying SCADA system, built upon raw information exchanged with SCADA appliances. Such raw information is transported upon the specific protocols supported by the abstracted devices, that's why SCADA adaptors deploy an Integration/Abstraction framework, that implements the required set of control and management protocols (MODBUS, IEC60780, SNMP etc.) to read/write SCADA devices statuses. Measurements, actuated control and command signals and other possibly CI technology dependent data from the SCADA system, which may be relevant for CI status assessment, are properly treated by the SCADA adaptor and sent to the IRP through the Secure Mediation Network.

Given the huge number of SCADA appliances that the Adaptor can abstract, the message formats, the data exchanged, and the message sequences differ case by case. Therefore we avoid to report MSC diagrams for this interface.

According to the Data Model maintained by the Adaptor, raw information exchanged are aimed to enrich a properly defined tree data structure, that describes objects and attributes. Examples of information exchanged are: nature of the abstracted devices, network physical ports and media, IP addresses, running services (FTP, SNMP, WS), supported protocols, error notifications, status data, logging info, messages to setup traps and timers inside the device, messages to operate a specific control on CI devices etc.

4.2.2 Detection Layer – CI Field interface

This interface is specified and realized within the development of the Detection Layer component (in particular, Task 3002, Task 3003 and Task 3005). The reader is referred to the documents describing the Detection Layer design [2] and the final version of the same document (currently in progress).

We recall that this interface is at the base of the activity of cyber-detection performed by the DL, which makes use of detection agents for CI networks, hosts and field devices activity and traffic monitoring. The portion of the DL directly interfacing with the CI includes local detection agents, honeypots, shadow RTUs, local HIDS and NIDS. All these components gather information from the CI (i.e. from the IT Network, the Operation Network and the Field Network) without interfering with CI operations and feed the DL modules devoted to cyber detection and reaction.

Examples of information exchanged are [2] traffic packets, input and outputs of field devices (e.g. input/outputs of RTUs acquired by a shadow RTU), system logs, registry keys, calls between applications and the operating system, etc.

4.2.3 Security Operator Human-Machine i/f (HMI)

The Security Operator Human-Machine (HMI) i/f enables the Security Operator to properly interact with the CockpitCI tool, with the purpose of:

1. Visualizing the cyber parameters (both current and predicted) related to the state of the CI and the suggested cyber reaction strategies in response to possible cyber threats;
2. Send cyber orders to the DL.

Therefore, the following three functionalities which need to be supported by the interface are the following:

1) *Visualize_Cyber-Parameter*, for visualization of the DL/IRP knowledge relevant to the cyber-security of the CI, like, for example, the current value (from the DL) or the predicted value (from the IRP) of a cyber-parameter.

2) *Suggest_Countermeasure*, for suggesting to the Security Operator (via the Security HMI) a countermeasure elaborated by the IRP in response to a cyber-threat.

3) *Send_Order*, allowing the Security Operator to send a cyber-order to the DL through the Security HMI.

4.2.3.1 Messages sequence chart diagrams

The number of cyber-parameters and quantities which may be relevant for the Security Operator knowledge is potentially very large in real cases. Therefore, it seems reasonable to assume that some main cyber parameters are displayed and updated continuously in time (i.e. with a high frequency), while some others are retrieved and visualized to the Security Operator on demand.

Figure 4-4 displays the MSC showing the single message of cyber-parameter update going from the DL to the Security operator. It is assumed that no acknowledgement of receipt is given by the Security Operator to the DL. This is because the visualization and the update of the main cyber-parameters is an activity performed continuously in time, and therefore it seems unrealistic to acknowledge on a continuous time-base (reasonably, it is only sufficient to have periodic check of HMI correct functioning).

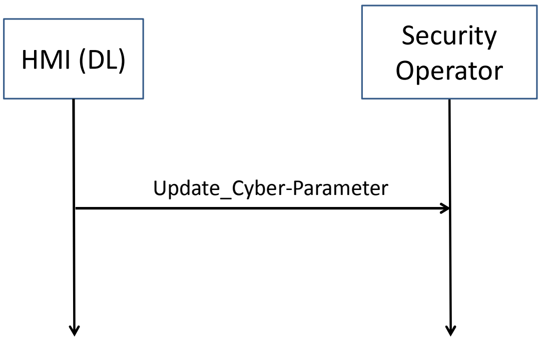


Figure 4-4 Visualize Parameter MSC

Figure 4-5 displays the MSC describing the request/reply process put in place whenever the Security Operator requires the visualization of a cyber-parameter which is not among the ones continuously displayed and updated.

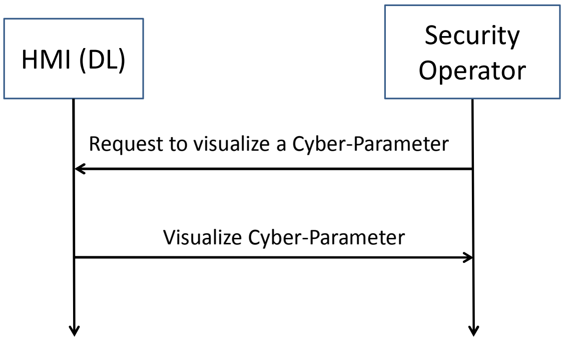

HMI (DL)
Security Operator
Request to visualize a Cyber-Parameter
Visualize Cyber-Parameter

Figure 4-5 Visualize Parameter MSC(on request).

The MSC in Figure 4-6 shows the interaction taking place between the DL and the Security Operator whenever a countermeasure (whether originating from the DL or coming from the IRP) is suggested by the former to the latter. In this case, given the timelines and the relevance of the message, it seems reasonable to consider an explicit acknowledgement from the Security Operator upon receiving of the countermeasure suggestion.

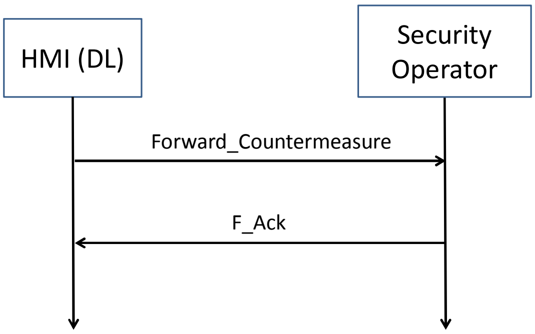


Figure 4-6 Suggest_Countermeasure MSC

Finally, the MSC in Figure 4-7 shows the interaction taking place between the DL and the Security Operator whenever a cyber-order is sent from the latter to the former. Also in this case it seems relevant to consider an explicit acknowledgement mechanism, which assures the Operator about the correct receipt of the command.

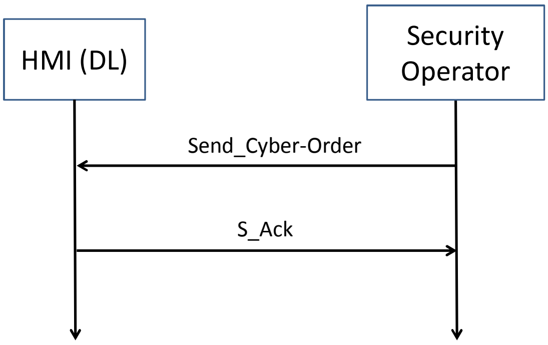


Figure 4-7: Send_Cyber-Order MSC.

4.2.3.2 Message descriptions

In the following we describe the messages exchanged between the actors and components mentioned above, supporting the functionalities identified for the Security Operator HMI i/f.

4.2.3.2.1 Update_Cyber-Parameter

This message is sent by IRP to the Security Operator through the Security HMI, with a proper timelines. The message may contain any DL/IRP knowledge that is valuable for the Security Operator. Possible parameters characterizing the message are given in the following table.

Parameter	Description
Predicted value of particular cyber-parameters	May be expressed as, e.g.: • Real/relative/natural numbers given according to a proper scale. • May be intuitively expressed on a colour scale (with proper acoustic/visual notifications in case of alarm values). • …
Cyber-security risk indicators	Risk indicators expressed according to a proper metric.

4.2.3.2.2 Request to visualize a Cyber-Parameter

This message is sent by the Security Operator to the DL trough the HMI, with the purpose of requesting the retrieval and the visualization of a particular cyber-parameter. The operation shall be intuitive for the Security Operator to carry out. The following parameters have to be considered.

Parameter	Description
Cyber-Parameter ID	Needed in order to univocally identify the parameter of interest. I may be a numerical or a textual ID.

4.2.3.2.3 Visualize a Cyber-Parameter

The message is sent by the DL to the Security Operator, via the HMI. It simply contains the information (which may be of numerical, textual, visual, etc. nature) associated to the requested cyber-parameter.

4.2.3.2.4 Forward_Countermeasure

The message is sent by the DL to the Security Operator. It contains a suggested countermeasure to be deployed in order to prevent cyber-attacks, mitigate their effect or react to them.

Parameter	Description
Rule ID	ID univocally identifying the rule (the suggested countermeasure).
Rule value	It contains the data specifying the suggested countermeasure (e.g. textual description, list of atomic operations, steps sequence, etc.).

4.2.3.2.5 F_Ack

Acknowledgement sent by the Security Operator to the DL, to notify that the countermeasure has been acquired and given full consideration.

Parameter	Description
Rule ID	ID univocally identifying the rule (the suggested countermeasure).
Result	The Operator acknowledges the correct receipt of the suggested countermeasure. The Operator may also inform the DL (according to proper timelines) whether the suggested countermeasure has been accepted or not (see also the next message description).

4.2.3.2.6 Send_Cyber-Order

Message sent by the Security Operator to the DL, in order to communicate a cyber-order.

Parameter	Description
Rule ID	ID univocally identifying the cyber-order (the suggested countermeasure).
Order	The cyber-order the Security Operator enters through the HMI. The order can be, e.g.: • Simple acceptance or rejection of a suggested counter-measure. • A change in DL settings. • A proper sequence of commands(maybe a subset of those suggested). • …

4.2.3.2.7 S_Ack

Message sent by the DL to the Security Operator in order to inform about the status (correct receipt, outcome, etc.) of the procedure.

Parameter	Description
Rule ID	ID univocally identifying the cyber-order (the suggested countermeasure).
Result	Information about the result of the cyber-order sending (e.g. failure of the procedure, successful completion of the procedure, etc.).

4.2.4 *SCADA Operator Human-Machine i/f (HMI)*

This external interface is fundamental for the SCADA Operator in order to access the IRP knowledge. The main functionality the interface has to support is therefore the visualization of messages coming from the IRP, including: predicted status of the CI (as assessed by IRP algorithms on the basis of collection of data from the field and mediation of information among linked CIs) and visualization of countermeasures suggested by the IRP to the SCADA Operator, to contrast threats resulting from cyber-attacks or faults. Therefore, the following two functionalities to be supported by the interface can be considered: 1) *Visualize_Service-Parameter*, for visualization of IRP knowledge, including for example the predicted value of service-parameters; 2) *Suggest_Countermeasure*, for suggesting to the SCADA Operator (via the HMI) a countermeasure elaborated by the IRP. The Operator decides whether to implement or reject the suggested reaction strategy. In case a reaction is put in place by the SCADA Operator, the resulting SCADA Orders will be sent to the actuating equipment through the SCADA Control Centre (i.e. it is not sent via this HMI). Nonetheless, the HMI between the SCADA Operator and the IRP is assumed to be bidirectional, in order to support additional interaction procedures (e.g. requests from the SCADA Operator to access to particular information in stored the IRP, acknowledgements from the SCADA Operator to particularly relevant IRP messages, etc.).

4.2.4.1 Messages sequence chart diagrams

MSCs are similar to the ones already presented for the Security Operator Human-Machine i/f (HMI). They are briefly recalled here for convenience.

Figure 4-8 refers to the process of continuous updating and visualization of a predicted operation parameter coming from the IRP.

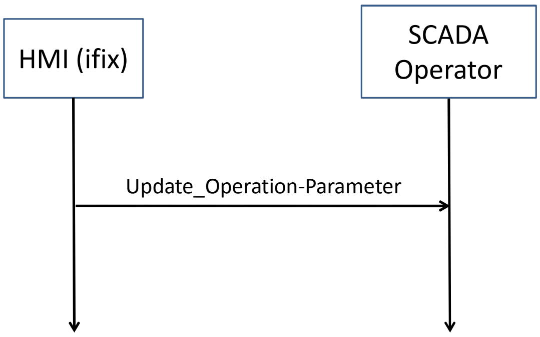


Figure 4-8: Continuous (i.e. with a proper frequency) IRP knowledge visualization.

Figure 4-9 instead refers to the process of IRP knowledge visualization based on a request/reply mechanism.

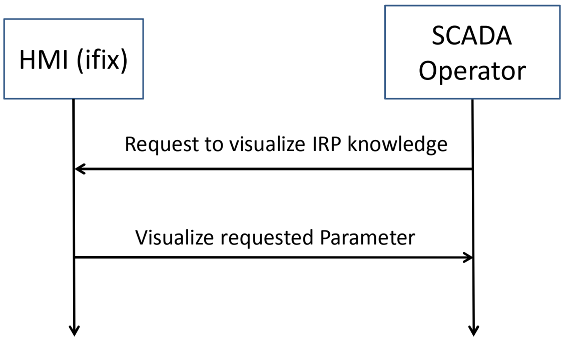

HMI (ifix)
SCADA Operator
Request to visualize IRP knowledge
Visualize requested Parameter

Figure 4-9: Request/reply mechanism for visualization of IRP knowledge.

Finally, Figure 4-10 is related to the process of forwarding a suggested countermeasure from the IRP to the SCADA Operator.

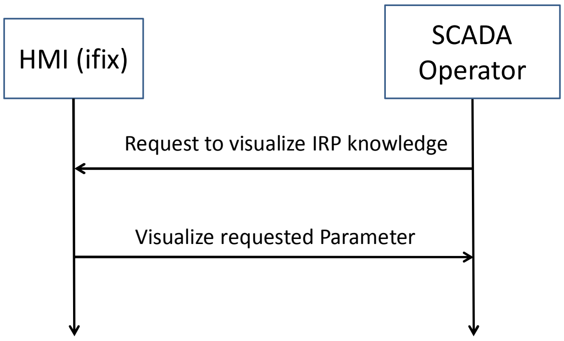

HMI (ifix)
SCADA Operator
Request to visualize IRP knowledge
Visualize requested Parameter

Figure 4-10: Suggested countermeasure visualization.

.

4.2.4.2 Message descriptions

4.2.4.2.1 Update_Operation_Parameter

This message is sent by the IRP to the SCADA Operator through the connecting HMI, with a proper timelines.

Parameter	Description
Information ID	Information for univocally identifying (in time, in space, etc.) the piece of exchanged information
Predicted value of particular oparation-parameters	May be expressed as, e.g.: • Real/relative/natural numbers given according to a proper scale. • May be intuitively expressed on a colour scale (with proper acoustic/visual notifications in case of alarm values). • …
Service indicators	Service indicators expressed according to a proper metric.

4.2.4.2.2 Request to visualize IRP knowledge

This message is sent by the SCADA Operator to the IRP trough the HMI, with the purpose of requesting the retrieval and the visualization of IRP knowledge. The operation shall be intuitive for the SCADA Operator to carry out. The following parameter has to be considered.

Parameter	Description
Information ID	Needed in order to univocally identify the knowledge of interest of the SCADA Operator. It may be a numerical or a textual ID.

4.2.4.2.3 Visualize a Requested Parameter

The message is sent by the IRP to the SCADA Operator, via the HMI. It simply contains the information (which may be of numerical, textual, visual, etc. nature) associated to the requested service-parameter.

4.2.4.2.4 Forward_Suggested_Countermeasure

The message is sent by the IRP to the SCADA Operator. It contains a suggested countermeasure to be deployed in order to react to menaces and possible service degradation resulting from cyber-attacks and/or faults affecting the infrastructure.

Parameter	Description
Rule ID	ID univocally identifying the rule (the suggested countermeasure).
Rule value	It contains the data specifying the suggested countermeasure (e.g. textual description, one or more lists of atomic operations to get out from the risk situation, steps sequence, consequences derived by the actuation of the suggested measures etc.).

4.2.4.2.5 F_Ack

Acknowledgement sent by the SCADA Operator to the IRP, to notify that the countermeasure has been acquired and given full consideration.

Parameter	Description
Rule ID	ID univocally identifying the rule (the suggested countermeasure).
Result	The Operator acknowledges the correct receipt of the suggested countermeasure. The Operator may also inform the IRP (according to proper timelines) whether the suggested countermeasure has been accepted or not.

4.2.5 SMN-Operator control interface

This interface exposes functionalities to enable the SMN management personnel (PE) to manage the gateway's status and configuration. Provided services include: SMN status checking, security policies configuration, retrieval of management information etc.

This section describes commands supported by the interface, and the protocol between the two communication end points supporting the aforementioned commands.

4.2.5.1 Messages sequence chart diagrams

This section describes interactions having place on the mentioned interface. Such interactions are aimed to support read/write operations on the gateway's status and configuration parameters. The interface does not support user sessions, therefore each operation performed by the PE is considered as an atomic operation. Such atomicity implies that each command invocation starts and ends respectively with the PE opening a new connection to the SMN, and the PE closing the previously opened connection, after that the command is executed. When the client PE opens the connection, he transmits both its credentials and the command to be executed. If the PE is authenticated and the command can be executed, then the connection is established and the command invocated. The following pictures Figure 4-11 provide sequence diagrams aimed to give an idea of the mentioned operations.

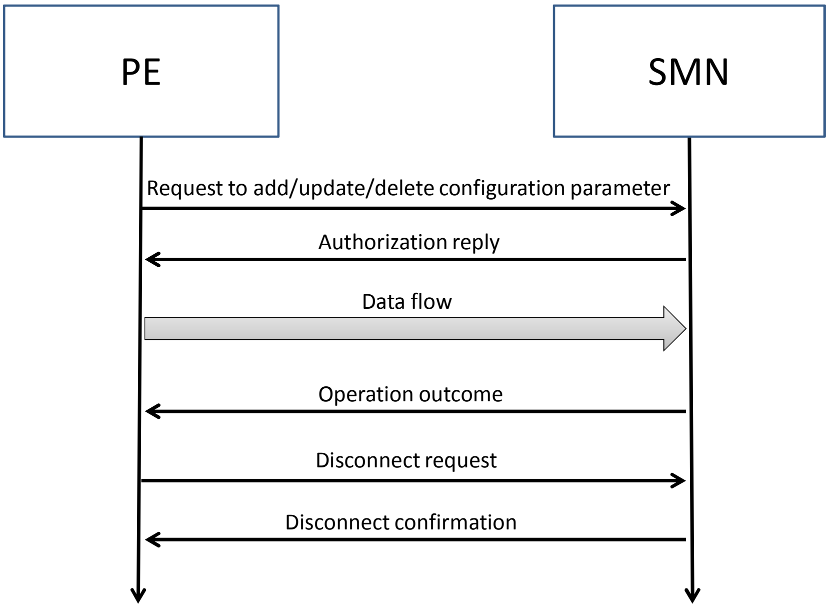


Figure 4-11: Write SMN configuration MSC.

As stated before, the interface that allows interaction with the SMN's configuration supports atomic transactions. This holds both for write and read functionalities. This is depicted in the picture above, where the PE needs before to establish a connection on the gateway's interface, issue the command, and then kill the connection. The same identical process takes place for the reading operation below. Figure 4-12

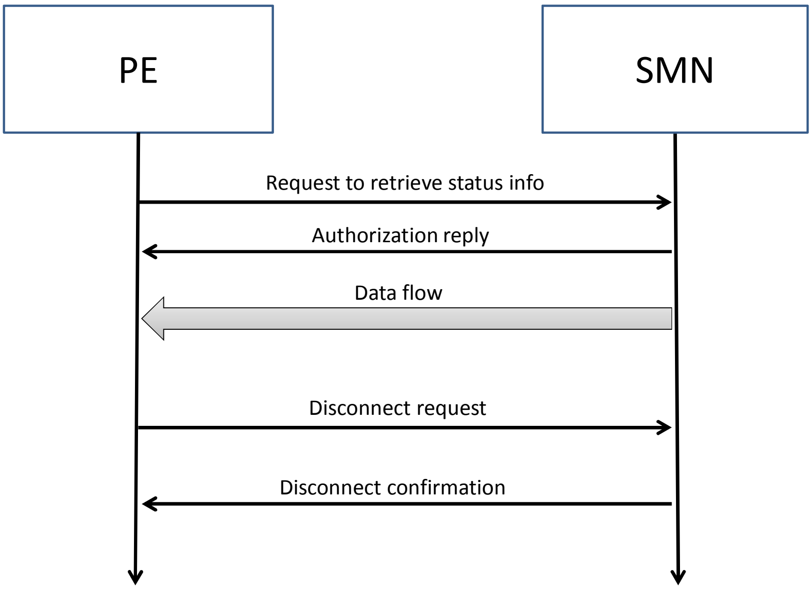


Figure 4-12: Read SMN configuration MSC.

In the next section a more detailed description of the exchanged messages is provided.

4.2.5.2 Message descriptions

Operations supported by the described interface are achieved by exchanging a certain number of messages. Such messages are described in the following subsections. A table is also provided to describe the information attached to each exchanged message.

4.2.5.2.1 Request to add/update/delete configuration parameter

This message is sent by the PE through the gateway's management console, to add, delete or modify the gateway's configuration. The following table provides a description of the call parameters.

Parameter	Description
Authentication ID	Credentials of the user that interacts with the service.
Action	Specifies the action to be executed (add, delete, modify).
Item ID	The ID of the item interested by the operation.

4.2.5.2.2 Authorization reply

Upon read/write request reception the external SMN replies with an acknowledgement message. The message content is explained below.

Parameter	Description
Request authorization	Tells whether the client is authenticated and the invoked operation can be performed. If exceptions rise up, this field is populated with error related information.

4.2.5.2.3 Operation outcome

After that PE performs the desired action on the selected configuration item, he is informed by the SMN of the operation outcome. Message details follow.

Parameter	Description
item ID	Item interested to the operation.
Result	Contains details about the performed action. In case of error this field specifies further details on the raised exception.

4.2.5.2.4 Request to retrieve status info

This message is generated when the gateway’s management PE performs a read access the SMN status. The status is represented by registered policies, and other information about the gateway’s internal functional elements. The interface supports different status access operations. The proper retrieval action to be performed is specified in a dedicated message field. The following table specifies call’s parameters.

Parameter	Description
Authentication ID	Credentials of the user that interacts with the service.
Action	Specifies type and format of the requested information (list items, deep items details, other status info listed with different rules)
Items list	It is the list of items to be accessed by the user, according to the previously specified actions.

4.2.5.2.5 Disconnect request

This message is generated by the management console to inform the gateway that the connection for the current action must be closed. The message does not contain parameters.

4.2.5.2.6 Disconnect confirmation

This message is sent back from the SMN to inform the manager that the connection is going to be closed. The message transports further information useful in case of error.

Parameter	Description
Result	Acknowledges the end of the connection. In case of error additional information can be found in this field.

4.2.6 SMN – SMN interface

This interface puts two peer SMNs into communication and allows the exchange of information between CIs over an untrusted network. This interface is supported by the Communication Engine and the Discovery Engine, both part of the SMN architecture. Services offered on this interface must be available over a well defined port and IP address in order to be reached by a peer SMN. Services offered on this interface are subject to policy restrictions that results in having peer gateways being not able to access full information, or being not allowed to access the service at all. The interface supports service discovery, service subscription/unsubscription and explicit information request (pull).

4.2.6.1 Messages sequence chart diagrams

This section describes interactions having place on the mentioned interface. Such interactions are aimed to spread CI information between interdependent CIs through their own SMNs. The exposed interface supports both synchronous and asynchronous communication patterns. The next sequence diagrams give an idea of the interactions taking place to support such communication.

The picture below Figure 4-13 reports a sequence diagram for the asynchronous communication scheme. The interaction starts with the client SMN (local) starting a service discovery toward a server SMN (external). The external gateway returns a list of discovered services (disclosed information set), which can be accessed by the local SMN accordingly to specified information access policies. At this point the local gateway submits a service subscription that must be approved by the server gateway. If the service subscription is approved, the external gateway is going to push its local data asynchronously to its subscriber, whenever updates are available. Subscription removal is up to the service subscriber (the client gateway), that invokes an unsubscription command on the interface. The unsubscription call is replied with a response message bringing the outcome of the call.

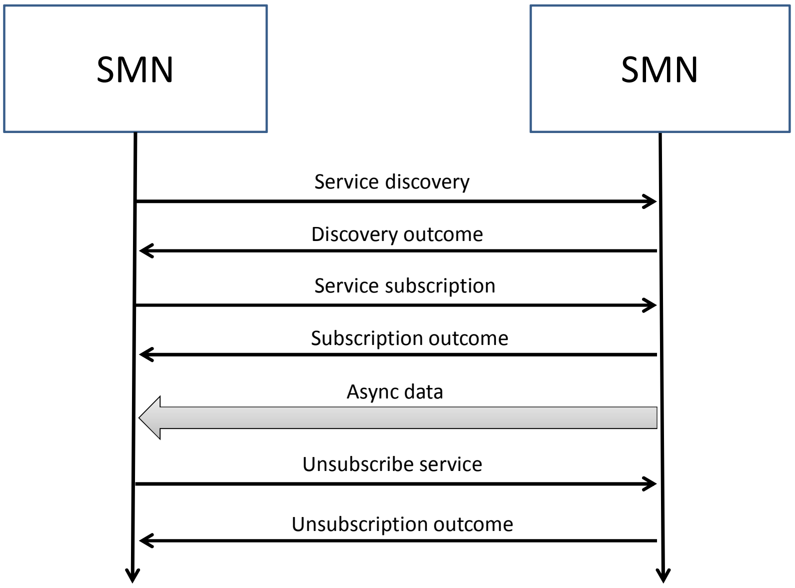


Figure 4-13: Asynchronous SMN-SMN communication MSC.

The second available communication scheme is based on a synchronous pattern. In this case no subscriptions are needed, but data are actively requested. The operation is atomic, and involves the local SMN opening and closing connections toward the external peer. The following picture Figure 4-14 gives more insights.

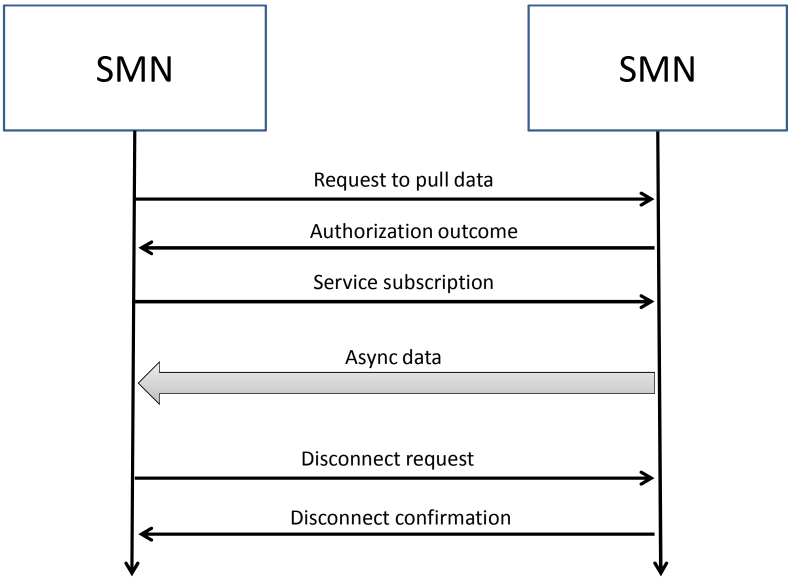


Figure 4-14: Synchronous SMN-SMN communication MSC.

4.2.6.2 Message descriptions

Operations supported by the described interface are achieved by exchanging a certain number of messages. Such messages are described in the following subsections. A table is also provided to describe the information attached to each exchanged message.

4.2.6.2.1 Service discovery

The subscription message is sent when a SMN wants to subscribe information relevant to another SMN. The table below describes the information carried in the message.

Parameter	Description
SMN ID	Identifier of the local SMN. This field is used by the external SMN for authentication and policy enforcement.

4.2.6.2.2 Discovery outcome

This is the message reply from the external SMN upon service discovery invocations. The table below describes the information carried in the message.

Parameter	Description
Request	Reports whether the requesting SMN is authenticated, and can

authorization	access published services.
Available services	List of services accessible by the requesting SMN, accordingly to its access policy restrictions.

4.2.6.2.3 Service subscription

The subscription message is sent when a SMN wants to subscribe information relevant to another SMN. The table below describes the information carried in the message.

Parameter	Description
SMN ID	Identifier of the subscribing SMN.
Service ID	The service to be subscribed.

4.2.6.2.4 Subscription outcome

When a subscription request is received, an acknowledgement message is generated, containing the information specified in the table below.

Parameter	Description
SMN_ID	Identifier of the external SMN.
Result	Contains subscription related information. In case of error this field specifies further details on the raised exception.

4.2.6.2.5 Unsubscribe

This message is sent whenever a subscriber SMN wants to unregister its subscription to an external SMN.

Parameter	Description
SMN_ID	Identifier of the SMN that performs the unsubscription.

4.2.6.2.6 Unsubscribe outcome

In response to the unsubscribe command, an acknowledgment is generated by the external SMN.

Parameter	Description

SMN_ID	Identifier of the external SMN.
Result	Brings information about the happened unsubscription. In case of error also brings information on the raised exception.

4.2.6.2.7 Request to pull data

This message is generated when a SMN wants to actively retrieve some peer's information. Since the call is request/response, the client SMN does not need to have a registered subscription by the peer gateway. Note that the pull command is atomic, and then this message is also aimed to authenticate the requesting counterpart.

Parameter	Description
SMN_ID	Identifier of the SMN that submits the request.
Information ID	Identifier of the needed information.

4.2.6.2.8 Authorization outcome

In response to a pull data request, an authorization message is generated, containing

Parameter	Description
Request authorization	Tells whether the local SMN is authenticated and the invoked operation can be performed. If exceptions rise up, this field is populated with error related information.

Disconnection messages are already described in this section, and are not repeated here to avoid duplication.

4.3 Internal interfaces

In this section the interfaces between internal sub-components of the CockpitCI tool (e.g. Integrated Risk Prediction Tool – Secure Mediation Network interface) are described.

- ***SMN – SCADA Adaptor i/f***: interface between the Secure Mediation Network and the SCADA adaptor.
- ***SMN – IRP tool i/f***: Interface between the Secure Mediation Network and the Integrated Risk Prediction Tool. It is used for data exchange with the local prediction tool. This interface must support bidirectional flow of data.

- ***SMN – PIDS i/f***: interface between the Secure Mediation Network and the PIDS. This interface must support bidirectional flow of data.

4.3.1 SMN – SCADA Adaptor interface

The SMN – SCADA Adaptor interface is an extension of the Adaptor – SMN interface already defined in the MICIE project [5]. In particular, contrary to the MICIE Adaptor-SMN standard interface, this standard interface must support bidirectional exchange of information, for allowing both flow of information from the SCADA control room to the IRP (and, possibly, to CI external authorized entities) and feedback of IRP knowledge to the SCADA control room, for enhancing detection and reaction capabilities. As already explained before, the interface is "standard" in the sense that it does not depend on the specific CI technology.

4.3.1.1 Messages sequence chart diagrams

Figure 4-15 describes an interaction between the SCADA Adaptor and the SMN aiming at storing new incoming data from the SCADA Control Centre to the Secure Mediation Network.

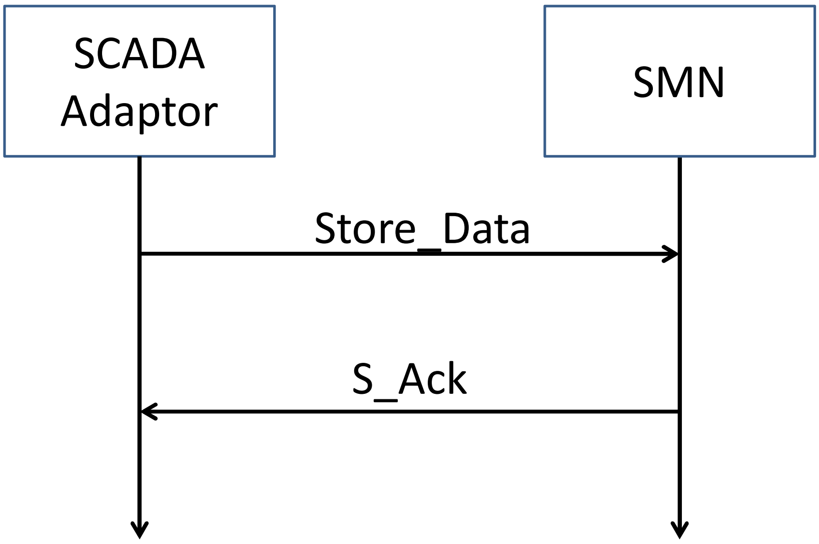


Figure 4-15 Store Data MSC

Figure 4-16 describes an interaction between the SCADA Adaptor and the SMN that aims to update an information already present in the SMN storage with a new incoming value.

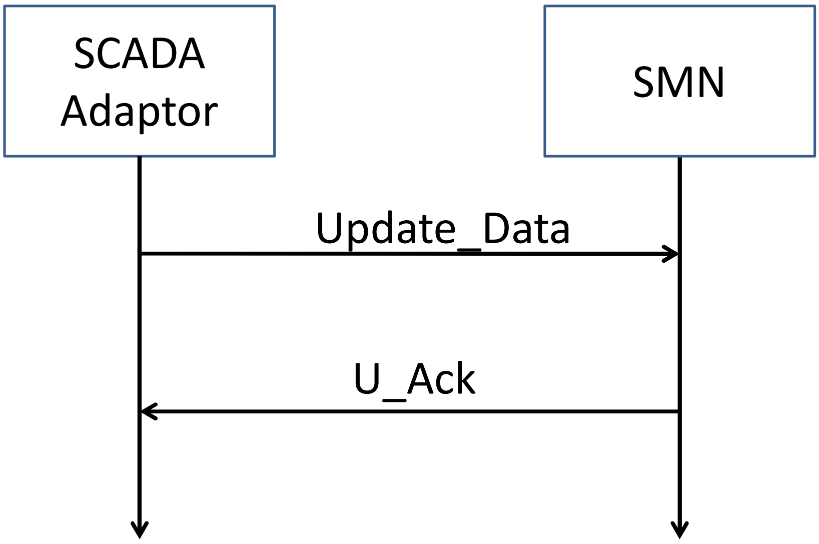


Figure 4-16 Update Data MSC

Figure 4-17 represents the exchange of information between the SCADA Adaptor and the SMN in order to propagate rules coming from the IRP regarding detection and reaction strategies updates to the SCADA Adaptor (that must forward this rules to the SCADA Operator.

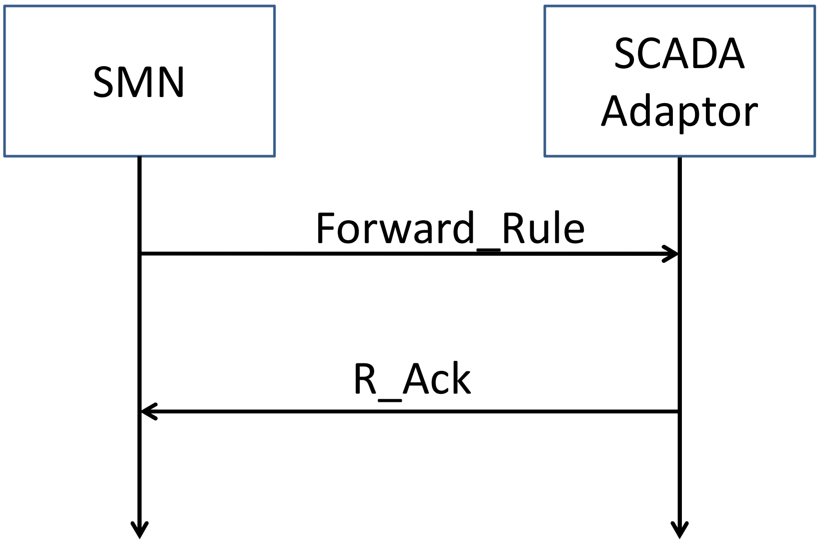


Figure 4-17 Forward Rule MSC

4.3.1.2 Message descriptions

4.3.1.2.1 Store_Data

This message is sent by the SCADA Adaptor to the SMN in order to store a new information into the SMN storage.

Parameter	Description
Data ID	Identifier of the new data/metadata to be stored in the DB
Value	It contains the data/metadata to be stored in the DB.

4.3.1.2.2 S_Ack

This message is sent by the SMN to the SCADA Adaptor in order to give feedback about the storing of the sent data.

Parameter	Description
Data ID	Identifier of the new data/metadata to be stored in the DB

Result	This field contains the result of the Store_Data procedure. Possible values are (i) a positive result (the data has successfully been stored into the SMN storage) or (ii) a negative result (the procedure encountered an error, further details on the error could be sent using this parameter).

4.3.1.2.3 Update_Data

This message is sent by the SCADA Adaptor to the SMN in order to update with a newest value an information already present In the SMN storage.

Parameter	Description
Message ID	Identifier of the Update_Data message. It should be a number that permits to uniquely identify the message.
Data ID	Identifier of the new data/metadata to be stored in the DB
Value	It contains the data/metadata to be stored in the DB.

4.3.1.2.4 U_Ack

This message is sent by the SMN to the SCADA Adaptor in order to give feedback about the storing of the sent data.

Parameter	Description
Data ID	Identifier of the new data/metadata to be updated in the DB
Result	This field contains the result of the Update_Data procedure. Possible values are (i) a positive result (the data has successfully been updated into the SMN storage) or (ii) a negative result (the procedure encountered an error, further details on the error could be sent using this parameter).

4.3.1.2.5 Forward_Rule

This message is sent by the SMN to the SCADA Adaptor in order to forward a rule coming from the IRP about a possible detection/reaction strategy to apply.

Parameter	Description
Rule ID	Identifier of the specific rule. It should be a number that permits to

	uniquely identify the rule.
Rule value	It contains a structured metadata describing the rule to be performed

4.3.1.2.6 R_Ack

This message is sent by the SCADA Adaptor to the SMN in order to give feedback about the forwarding of the detection/reaction rule.

Parameter	Description
Rule ID	Identifier of the rule.
Result	This field contains the result of the Forward Rule procedure. Possible values are (i) a positive result (the rule has successfully been forwarded to the SCADA Adaptor) or (ii) a negative result (the procedure encountered an error, further details on the error could be sent using this parameter).

4.3.2 SMN – IRP tool interface

The SMN – IRP interface is an extension of the SMN – PT (Prediction Tool) interface defined in the MICIE project [5]. The SMN – IRP interface enables the communication between the Secure Mediation Network and the Integrated Risk Predictor. The IRP could use this interface to ask for a specific information stored in the SMN in order to perform its operations. Nevertheless the IRP also uses this interface in order to propagate the result of its operations to the SMN making them available for external peer IRPs and for local modules (e.g. the SCADA Operator about detection/reaction strategies). The SMN – IRP interface is bidirectional and it is used by the SMN to send information to the IRP.

4.3.2.1 Messages sequence chart diagrams

Figure 4-18 describes a subscription operations. In particular, the IRP could subscribe to a specific information made available from the SMN in order to be update whenever this information changes.

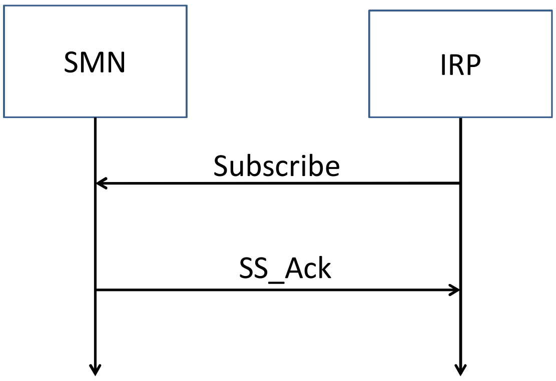


Figure 4-18 Subscribe MSC

Figure 4-19 describes, similarly to the previous MSC, an un-subscription operation, performed by the IRP when it is no more interested to a previously subscribed information med available from the SMN.

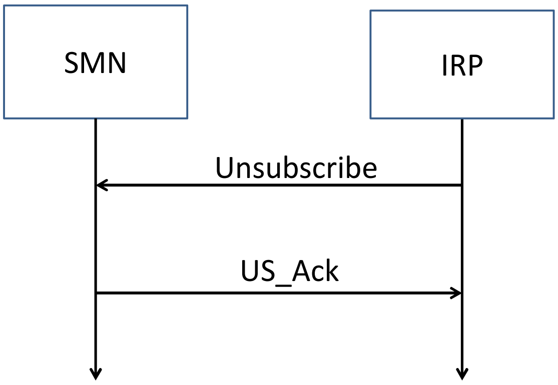


Figure 4-19 Unsubscribe MSC

When the IRP is subscribed to a specific information it could receive updates from the SMN. This paradigm is represented in Figure 4-20.

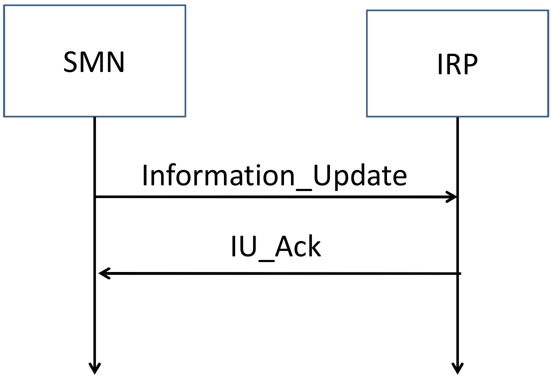


Figure 4-20 Information Update MSC

The IRP periodically perform its prediction operations. Whenever e new prediction result is available the IRP needs to store it on the SMN in order to make it available to other interdependent IRPs deployed in other CIs. This operation is described in Figure 4-21.

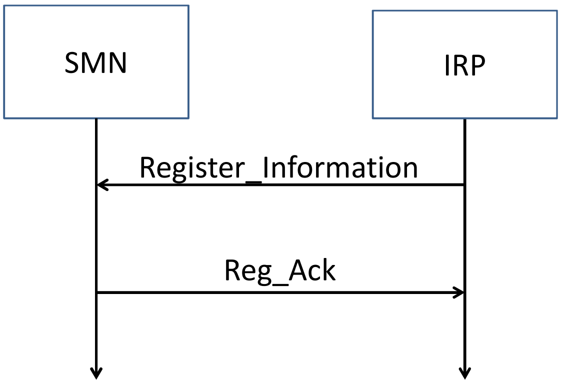


Figure 4-21 Register Information MSC

Figure 4-22 represents the de-registration procedure. This procedure is used by the IRP when it has to de-register a previously registered information on the SMN.

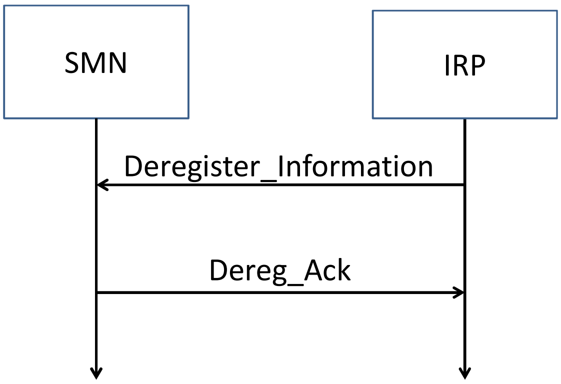


Figure 4-22 Deregister Information MSC

The IRP is allowed to update a previously registered information on the SMN by means of the procedure described in Figure 4-23.

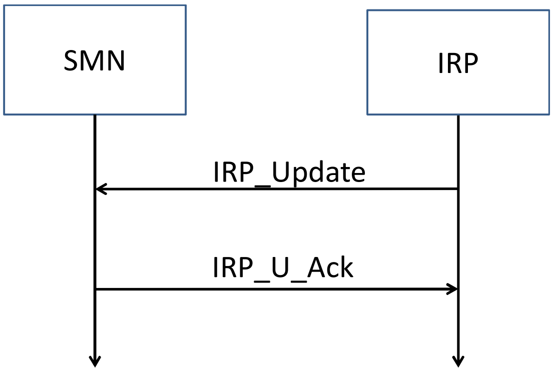


Figure 4-23 IRP Update MSC

The SMN – IRP interface is also used by the IRP to forward information about detection/reaction strategies destined to the SCADA Operator. This paradigm is described in Figure 4-24.

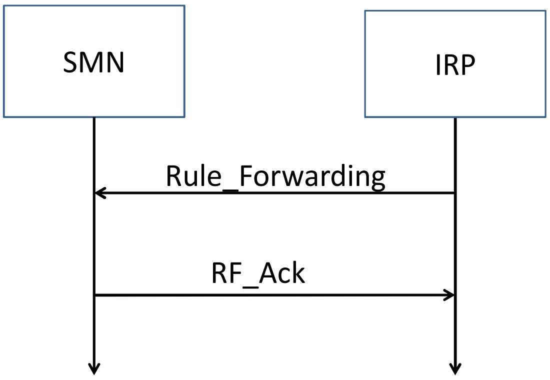


Figure 4-24 Rule Forwarding MSC

4.3.2.2 Message descriptions

4.3.2.2.1 Subscribe

This message is sent by the IRP to the SMN in order to inform the SMN to send all updates related to this specific information.

Parameter	Description
Information ID	Identifier of the specific information

4.3.2.2.2 SS_Ack

This message is sent by the SMN to the IRP in order to inform it about the outcome of the subscribe operation.

Parameter	Description
Information ID	Identifier of the specific information
Result	It contains information about the result of the subscription. In case the subscription fails, further details on the error could be sent using this parameter.

4.3.2.2.3 Unsubscribe

This message is sent by the IRP to the SMN in order to unsubscribe to the updates of the specific information.

Parameter	Description
Information ID	Identifier of the needed information

4.3.2.2.4 US_Ack

This message is sent by the SMN to the IRP in order to inform it about the outcome of the unsubscribe operation.

Parameter	Description
Information ID	Identifier of the specific information
Result	It contains information about the result of the un-subscription. In case the un-subscription fails, further details on the error could be sent using this parameter.

4.3.2.2.5 Information_Update

This message is sent by the SMN to the IRP in order to inform it about a new update value of a subscribed information.

Parameter	Description
Information ID	Identifier of the specific information
Value	It contains the updated value of the information.

4.3.2.2.6 IU_Ack

This message is sent by the IRP to the SMN in order to inform it about the outcome of the information update operation.

Parameter	Description
Information ID	Identifier of the specific information
Result	It contains information about the result of the information update operation. In case the operation fails, further details on the error could be sent using this parameter.

4.3.2.2.7 Register_Information

This message is sent by the IRP to the SMN in order to register a specific information.

Parameter	Description
Information ID	Identifier of the information to be registered.

4.3.2.2.8 Reg_Ack

This message is sent by the SMN to the IRP in order to inform it about the outcome of the register information operation.

Parameter	Description
Information ID	Identifier of the specific information
Result	It contains information about the result of the register information operation. In case the operation fails, further details on the error could be sent using this parameter.

4.3.2.2.9 Deregister_Information

This message is sent by the IRP to the SMN in order to deregister a specific information

Parameter	Description
Information ID	Identifier of the information to be deregistered.

4.3.2.2.10 Dereg_Ack

This message is sent by the SMN to the IRP in order to inform it about the outcome of the deregister information operation

Parameter	Description
Information ID	Identifier of the specific information
Result	It contains information about the result of the deregister information operation. In case the operation fails, further details on the error could be sent using this parameter.

4.3.2.2.11 IRP_Update

This message is sent by the IRP to the SMN in order to update the value of a specific information previously registered.

Parameter	Description

Information ID	Identifier of the information to be updated.
Value	It contains the updated value of the information.

4.3.2.2.12 IRP_U_Ack

This message is sent by the SMN to the IRP in order to inform it about the outcome of the IRP update operation

Parameter	Description
Information ID	Identifier of the specific information
Result	It contains information about the result of the IRP update operation. In case the operation fails, further details on the error could be sent using this parameter.

4.3.2.2.13 Rule Forwarding

This message is sent by the IRP to the SMN in order to forward a specific detection/reaction rule toward the local SCADA Operator.

Parameter	Description
Rule ID	Identifier of the specific rule to be forwarded.
Value	It contains the updated value of the information.

4.3.2.2.14 FR_Ack

This message is sent by the SMN to the IRP in order to inform it about the outcome of the rule forwarding operation.

Parameter	Description
Rule ID	Identifier of the specific rule.
Result	It contains information about the result of the rule forwarding operation. In case the operation fails, further details on the error could be sent using this parameter.

4.3.3 SMN – PIDS interface

The interface between the Secure Mediation Network and the Detection Layer enables also the logical communication between the DL and the IRP. All communication flows between CockpitCI system sub-components, in fact, physically passes through the SMN. In this respect, this interface is bidirectional and the main information flows it admits are described in the followings paragraphs.

4.3.3.1 Messages sequence chart diagrams

The following Figure 4-25 describes a subscription operations. In particular, the DL could subscribe to a specific information made available from the SMN in order to be update whenever this information changes. In particular these information may relate to new automatic countermeasures in the context of cyber risk provided from the IRP.

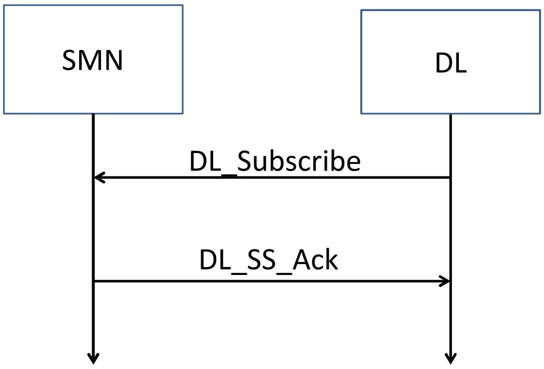


Figure 4-25 DL Subscribe MSC

The following Figure 4-26 describes, similarly to the previous MSC, an un-subscription operation, performed by the DL when it is no more interested to a previously subscribed information med available from the SMN.

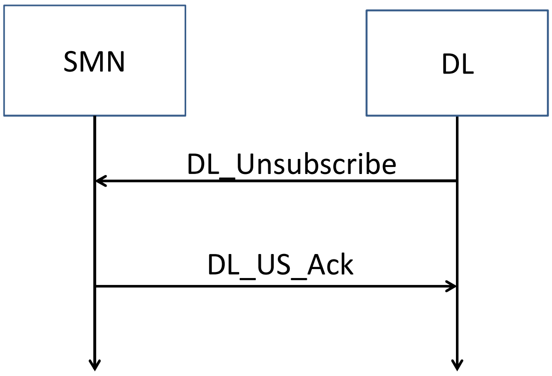


Figure 4-26 Unsubscribe MSC

When the DL is subscribed to a specific information it could receive updates from the SMN. This paradigm is represented in the following Figure 4-27.

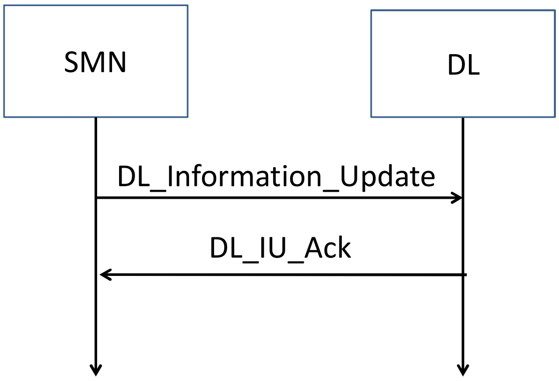


Figure 4-27 Information Update MSC

The DL performs its cyber operations, continuously producing cyber detection parameters. Whenever e newly calculated cyber detection parameters are available, the DL need to store them on the SMN in order to make it available to the local IRP deployed in the local CI. This operation is described in the following Figure 4-28.

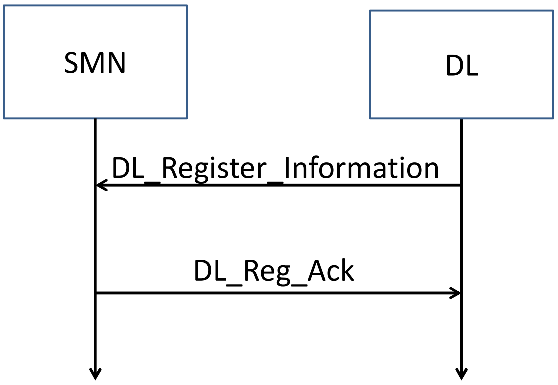


Figure 4-28 Register Information MSC

The following Figure 4-29 represents the de-registration procedure. This procedure is used by the DL when it has to de-register a previously registered information on the SMN.

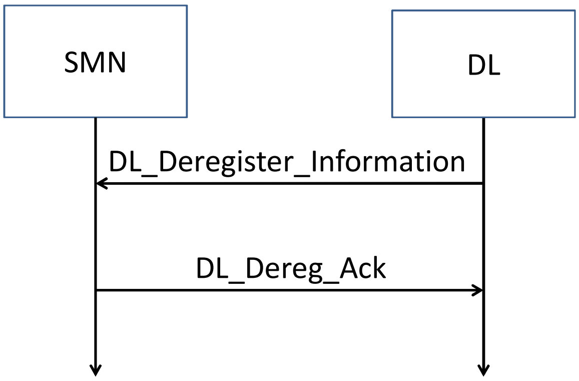


Figure 4-29 Deregister Information MSC

The DL is allowed to update a previously registered information on the SMN by means of the procedure described in the following figure.

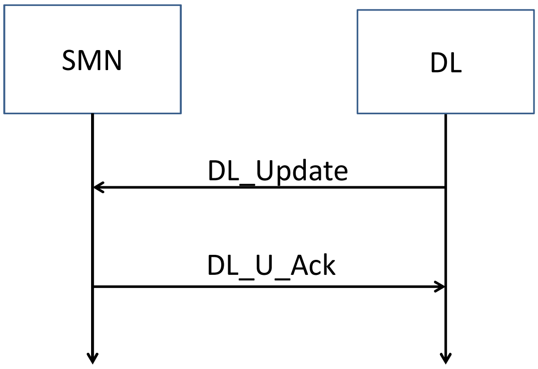


Figure 4-30 DL Update MSC

4.3.3.2 Message descriptions

4.3.3.2.1 DL_Subscribe

This message is sent by the DL to the SMN in order to inform the SMN to send all updates related to this specific information.

Parameter	Description
Information ID	Identifier of the specific information

4.3.3.2.2 DL_SS_Ack

This message is sent by the SMN to the DL in order to inform it about the outcome of the subscribe operation.

Parameter	Description
Information ID	Identifier of the specific information
Result	It contains information about the result of the subscription. In case the subscription fails, further details on the error could be sent using this parameter.

4.3.3.2.3 DL_Unsubscribe

This message is sent by the DL to the SMN in order to unsubscribe to the updates of the specific information.

Parameter	Description
Information ID	Identifier of the needed information

4.3.3.2.4 DL_US_Ack

This message is sent by the SMN to the DL in order to inform it about the outcome of the unsubscribe operation.

Parameter	Description
Information ID	Identifier of the specific information
Result	It contains information about the result of the unsubscription. In case the unsubscription fails, further details on the error could be sent using this parameter.

4.3.3.2.5 DL_Information_Update

This message is sent by the SMN to the DL in order to inform it about a new update value of a subscribed information (e.g. a newly stored automatic countermeasure).

Parameter	Description
Information ID	Identifier of the specific information
Value	It contains the updated value of the information.

4.3.3.2.6 DL_IU_Ack

This message is sent by the DL to the SMN in order to inform it about the outcome of the information update operation.

Parameter	Description
Information ID	Identifier of the specific information
Result	It contains information about the result of the information update operation. In case the operation fails, further details on the error could be sent using this parameter.

4.3.3.2.7 DL_Register_Information

This message is sent by the DL to the SMN in order to register a specific information (e.g. newly calculated cyber detection parameters).

Parameter	Description
Information ID	Identifier of the information to be registered.

4.3.3.2.8 DL_Reg_Ack

This message is sent by the SMN to the DL in order to inform it about the outcome of the register information operation.

Parameter	Description
Information ID	Identifier of the specific information
Result	It contains information about the result of the register information operation. In case the operation fails, further details on the error could be sent using this parameter.

4.3.3.2.9 DL_Deregister_Information

This message is sent by the DL to the SMN in order to deregister a specific information

Parameter	Description
Information ID	Identifier of the information to be deregistered.

4.3.3.2.10 DL_Dereg_Ack

This message is sent by the SMN to the DL in order to inform it about the outcome of the deregister information operation

Parameter	Description
Information ID	Identifier of the specific information
Result	It contains information about the result of the deregister information operation. In case the operation fails, further details on the error could be sent using this parameter.

4.3.3.2.11 DL_Update

This message is sent by the DL to the SMN in order to update the value of a specific information previously registered.

Parameter	Description
Information ID	Identifier of the information to be updated.
Value	It contains the updated value of the information.

4.3.3.2.12 DL_U_Ack

This message is sent by the SMN to the DL in order to inform it about the outcome of the IRP update operation

Parameter	Description
Information ID	Identifier of the specific information
Result	It contains information about the result of the IRP update operation. In case the operation fails, further details on the error could be sent using this parameter.

5 CockpitCI HMI

This section addresses the tool interface (HMI) towards the SCADA and the ICT Operator. It is interesting to extract some remarks which were made by the end-users in the End-User Questionnaire, which is appended at the end of D5.1[1]. Regarding SCADA and cyber operators, the questionnaires reports the following answers:

- *2 different teams with different goals (one is to operate the CI and another to prevent cyber attacks). ……. 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 …….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;*
- *….in our organization security and SCADA operator already cooperate to reduce cyber threats …their knowledge differs……need to exchange information efficiently……;*
- *…intuitive interfaces……*

The CockpitCI tool should be envisaged as an automatic tool which may support the Operators and which also allows their interaction to be held at a higher level of abstractions. The HMI should provide each Operator a comfortable view of the CI environment but also provide a bridge between the two views so as to facilitate collaboration and coordination. A preliminary list of the information which should be presented to each Operator is the following:

<u>ICT Operator</u>:

- cyber status of ICT network and its near-term evolution due to cyber attack;
- which ICT equipment and/or ICT services are at risk due to propagation of cyber attack and corresponding risk level;
- which ICT equipment and/or service is most important for maintaining CI QoS;
- Suggested countermeasures.

<u>SCADA Operator</u>:

- SCADA impacted services;
- Risk assessment;
- Suggested countermeasures.

In the following we also depict three possible dialogues between the SCADA operator and the ICT Operator.

The first vignette highlights how the prediction capability of the tool and the awareness of what might happen in the near future can support the Operators in taking better decisions (e.g. in this case it may be better not to rely on Power Station X so as to limit the propagation of the cyber attack).

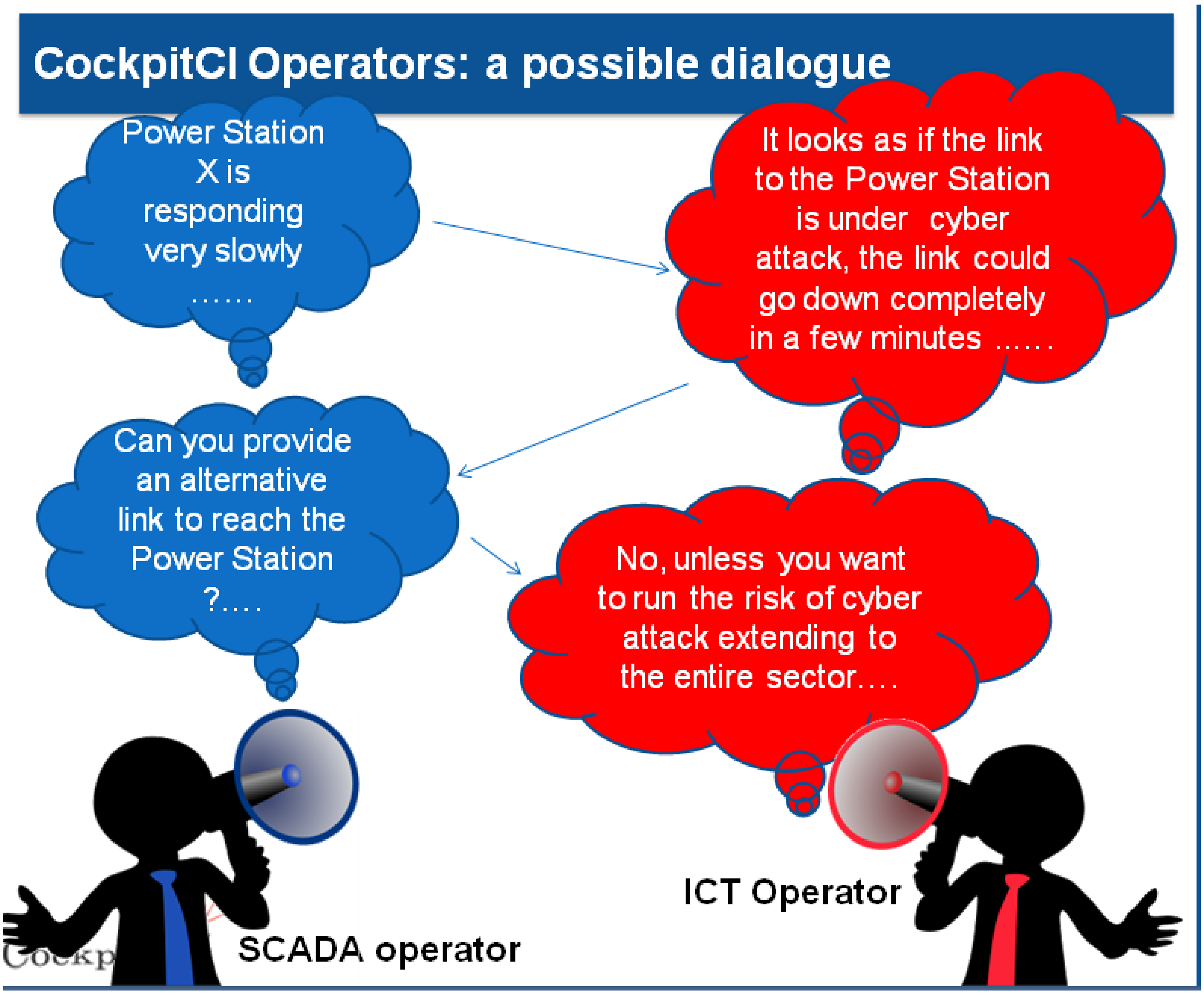
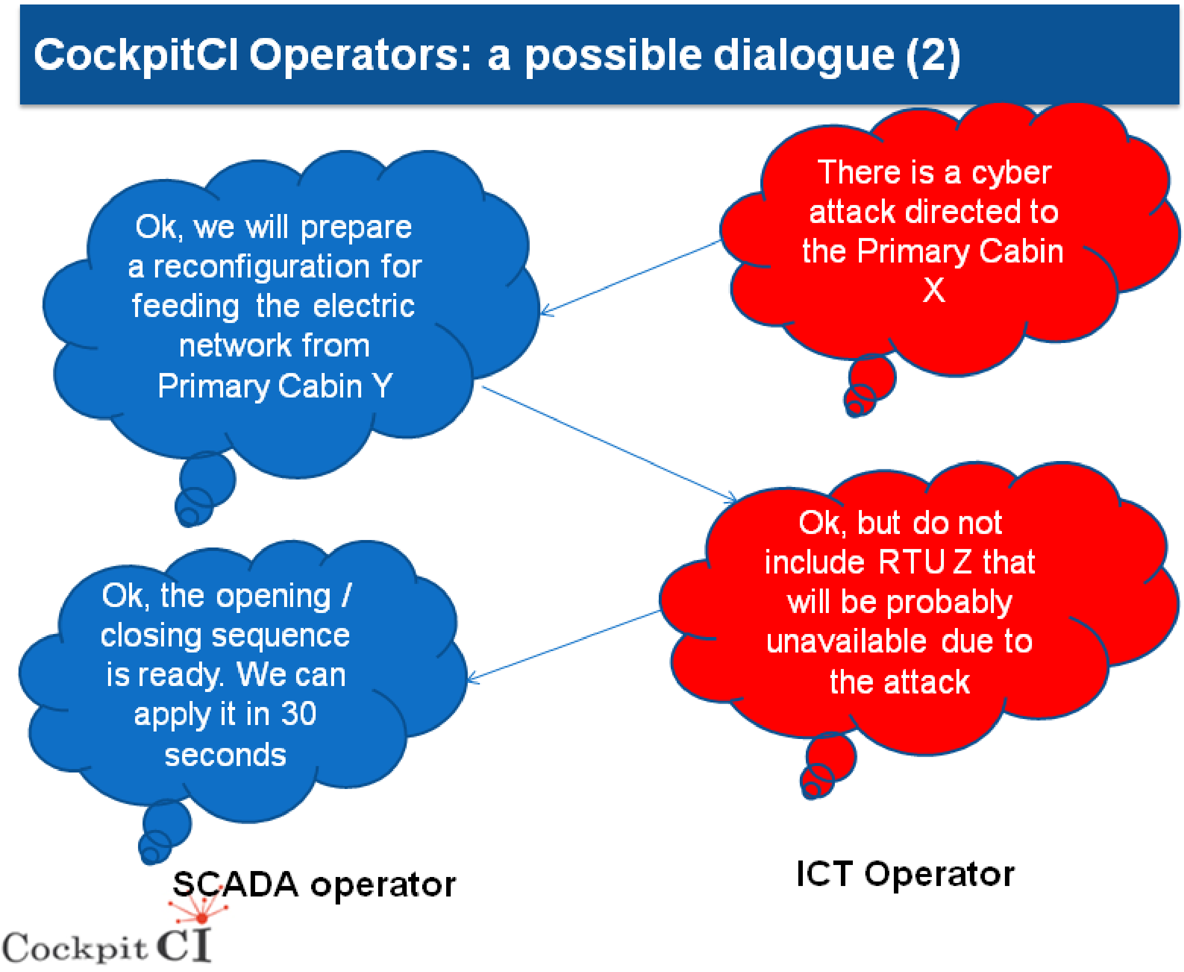

CockpitCI Operators: a possible dialogue
Power Station X is responding very slowly ……
It looks as if the link to the Power Station is under cyber attack, the link could go down completely in a few minutes ……
Can you provide an alternative link to reach the Power Station ?….
No, unless you want to run the risk of cyber attack extending to the entire sector….
ICT Operator
SCADA operator

Figure 5-1 Dialogue 1

The second vignette highlights how the dialogue is performed at a high operative level and how the ICT Operator is managing to make reference to entities (e.g. Primary Cabin , RTU) which are familiar to the SCADA operator (i.e. mapping his cyber information in a SCADA perspective). In this case the cyber detection and analysis capability of the tool and also the capability to propagate ahead in time the effects of the cyber attack are essential to support the Operators in taking the right decision.



CockpitCI Operators: a possible dialogue (2)

There is a cyber attack directed to the Primary Cabin X

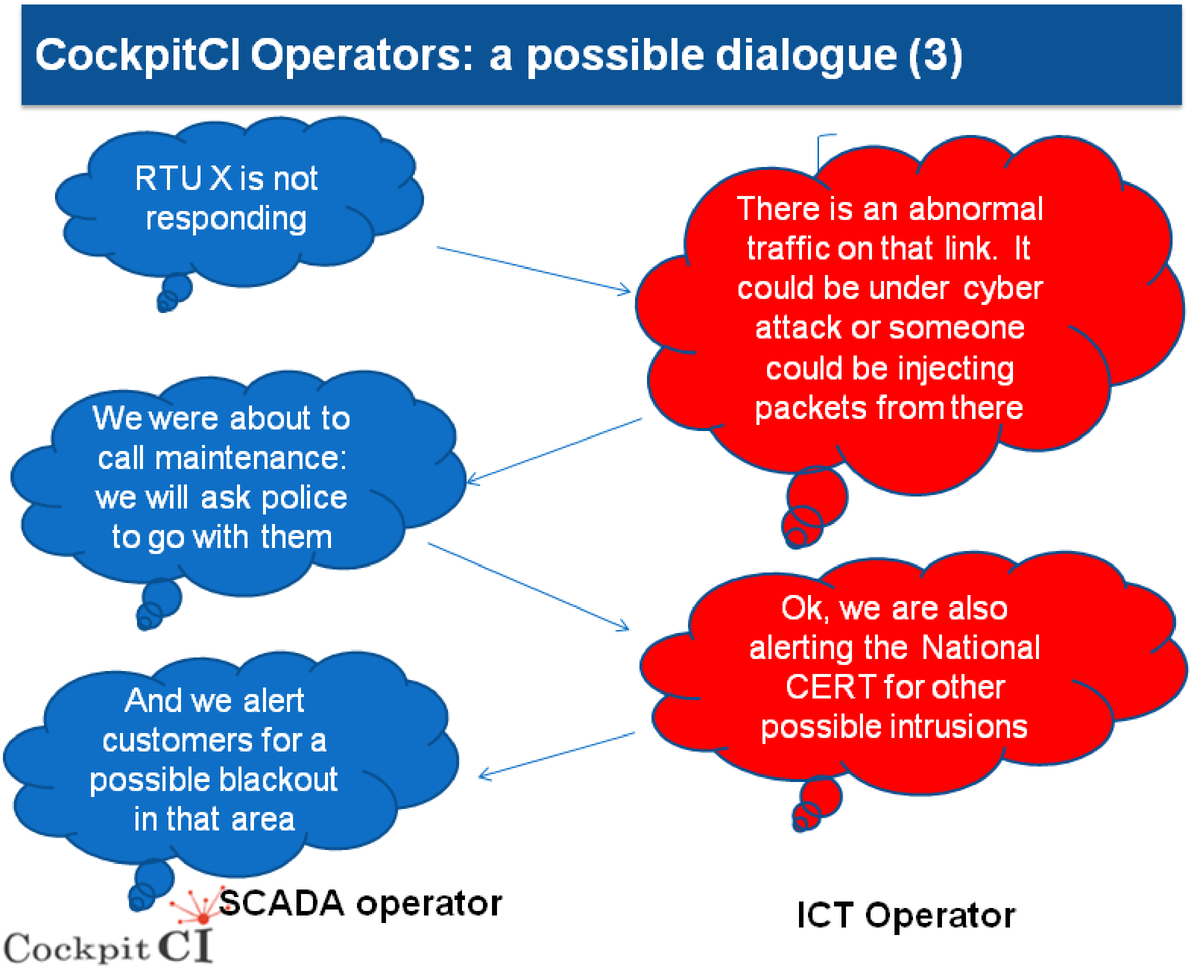
Ok, we will prepare a reconfiguration for feeding the electric network from Primary Cabin Y

Ok, but do not include RTU Z that will be probably unavailable due to the attack

Ok, the opening / closing sequence is ready. We can apply it in 30 seconds

Figure 5-2 Dialogue 2

The third vignette highlights how the tool may ease and support connectivity towards other parties and produce a much more effective and rapid response to the cyber threat.



CockpitCI Operators: a possible dialogue (3)

RTU X is not responding

There is an abnormal traffic on that link. It could be under cyber attack or someone could be injecting packets from there

We were about to call maintenance: we will ask police to go with them

Ok, we are also alerting the National CERT for other possible intrusions

And we alert customers for a possible blackout in that area

Figure 5-3 Dialogue 3

6 Security

The security of the CockpitCI tool is an important issue and one of the first which gets raised in a discussion regarding the feasibility of the tool or presentation to potential end-users. Yet the security of the tool is not the purpose of this project. The purpose of the project is “a proof of concept”, i.e. that it is possible to gain a higher situation awareness by including the cyber factor in the picture, and also that it is possible to either support the Operator in making the best decision or rather trigger automatic reactions at the central or local level.

The concern of the security of the CockpitCI tool should be handled similarly as to when new security software (e.g. IDS, IPS,..) is added to the system architecture.

The CockpitCI tool can be designed at the state-of-the-art of security: this is a certainly different situation when compared to many legacy SCADA systems which were designed with no consideration about security issues. The CockpitCI tool can also be maintained at the state-of-the-art of security: new software and patches can be installed more easily and rapidly, since it does not directly affect the plant operation (at least in the monitoring configuration); this is a certainly different situation when compared to many legacy SCADA systems where patching and software update is not performed so as not to interrupt the business process.

The CockpitCI tool is in principle exposed to cyber attacks and therefore it may provide inaccurate/false information to system operators, either to disguise unauthorized changes or to cause the operator to initiate inappropriate actions. The main intrusion paths are the following:

- via the external interfaces, especially the SMN interface towards other CIs which is an external world interface towards the Internet;
- via the Detection Layer since it collates information from the field where also physical security is a problem; two types of attacks could be initiated through this path, either DOS attacks to make the CockpitCI System unavailable by sending false mass information to system or smart attacks which misuse the tools by sending false but coherent information;
- insiders as no one security system is fully protected against malicious attacks initiated inside the system by malicious users or manipulated users (social hacking): e.g. the most probable penetration vector of Stuxnet attack on Iranian Nuclear plant was a infected mobile device (USB key).

Any additional piece of software and hardware can introduce vulnerabilities; and this occurs for CockpitCI tool as well, its introduction will inevitably raise new vulnerabilities into the overall system. The design of the system must ensure that the vulnerabilities introduced are minimal. In addition what needs to be addressed is the risk trade-off: if we can demonstrate that the potential advantages of a tool like CockpitCI are higher than the corresponding increase in cyber-risk, then the job is done. Today nobody in the IT domain would dream not to install a firewall or an IPS because of security concerns.

According to requested system designed in the present document (see above), the preliminary security architecture to deploy the CockpitCI system should be set up as designed in following figure. This preliminary schema can of course be re-evaluated according to users requirements.

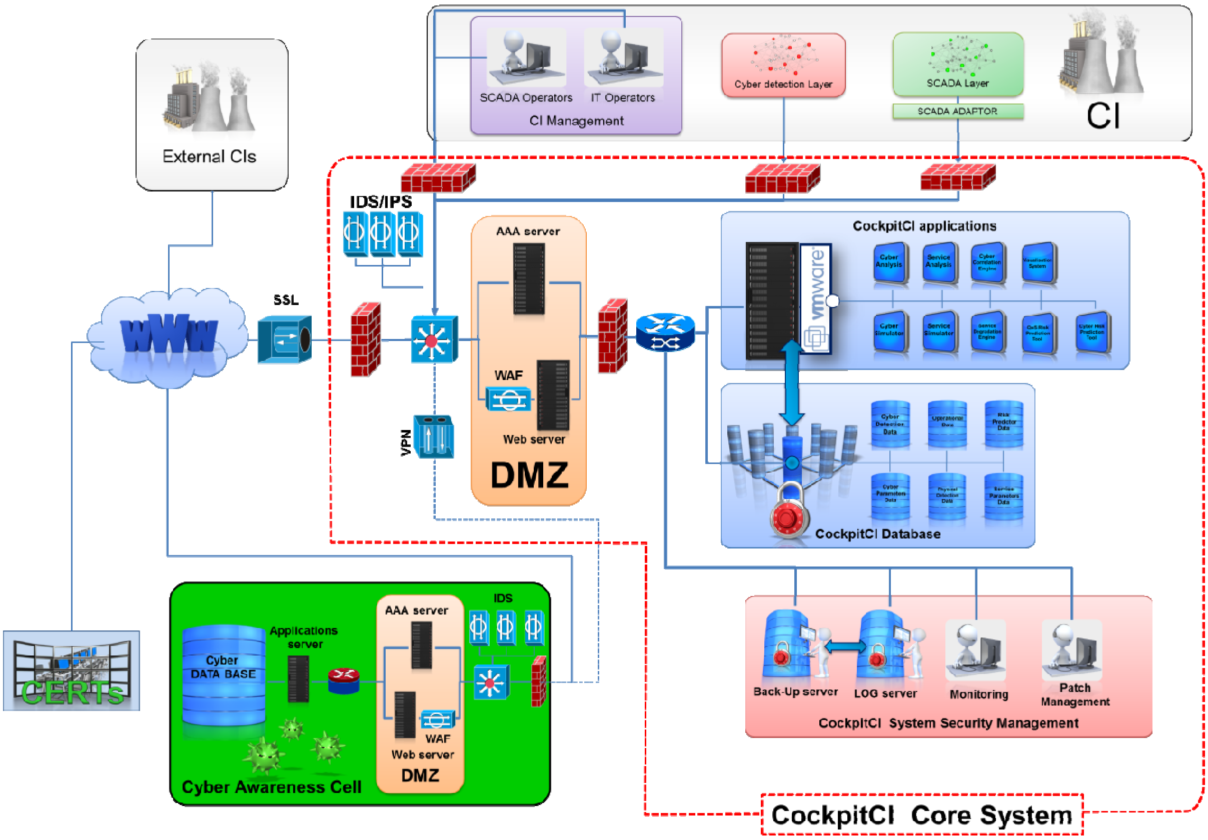


Figure 6-1 Preliminary schema of secure deployment of CockpitCI Core System

The figure describes a security architecture which allows to protect the core system in a secure area. The main security measures designed are:

- The paths with external sources coming from internet, from detection (cyber and SCADA) layers, or from CI operators' consoles are not directly interconnected to the core system but are controlled in a DMZ area by firewalling, AAA (authentication, authorization and Accounting) server and IPS/IDS systems (able to control traffic data flow according to used protocols).
- The protocol used to connect to the system from the internet area is a secure protocol as SSL.
- As the easiest way to connect to the CockpitCI system is a web service, the DMZ includes a web server protected by WAF (Web Application Firewall) which controls the data flow and user requests at a finer granularity with respect to the firewall.
- The CockpitCI Tools are deployed behind another firewall to avoid direct access to applications or database servers.

- The applications would be deployed in virtual servers' system to enforce the reliability and the versatility of the system and to allow an easy up-scaling in a production phase.
- The whole set of CockpitCI database will be hosted in dedicated data servers farms (silo containment) to be able to control the access to every data according to users policies and all data will be stored in safe manner (e.g. encrypted database).
- The Cyber awareness cell (part of public or private CERT or of a CIs laboratory) which has the objective to analyze more deeply the unidentified cyber threats (but already detected as abnormal activities), will be designed on the same security schema and linked to the CockpitCI system either through the common internet path (SSL protocol) or through a dedicated VPN line.

Even if the CockpitCI system will be a first design as a POC, it is important to design, at this step, the security management layer of the tool in order to provide a system according to the best practice of security design. In that aim the system should include:

- A Log server to store all activities performed (management activity, traffic activity, database modification etc…).
- A monitoring cell to control the functioning of the system and monitor the security devices (as firewall, IDS/IPS etc).
- A patch management cell which could perform the secure updating of the whole system in case of security incident or regular maintenance.
- A Back-up server to ensure a Business Continuity Management of the system. As CockpitCI aims to be a control system and does not target a high availability level, a simple solution of back-up to store a copy of the data-base, VM images etc… could be enough to ensure the targeted availability level. The RPO (Return Point Objective), which is the point from which it is possible to recover the whole data from back-up, shall be fixed according to users requirements.

Last but not least, attention should be paid to two points in security management to design the CockpitCI system:

1. The first one is the definition and implementation of security policies according to user requirements. This point deals especially with the firewalling policies and access policies to data and applications.
2. The second one is to design and implement the entire system in order to provide a high security assurance level. This point could be reached by:
    a. Use commercial devices with a high security assurance level such as devices certified EAL4+ or higher in the ISO 15408 rating scale.
    b. Test the vulnerabilities of the final POC by performing first code reviews according to best practices guideline (as for example OWASP web application guideline), and secondly penetration testing of the final solution in blind or not-blind approach.
    c. Enable a management of the system based on an improvement cycle such as PDCA (Plan Do Check Act) cycle.

7 Conclusions

This deliverable puts together the building blocks of the CockpitCI, namely the Detection Layer, the Secure Mediation Network and the Integrated Risk Predictor, and provides an insight of how these components should work together in order to handle security incidents and their treatment and achieve project objectives. For this reason the information flow and a detailed functional diagram is provided, showing the processing steps performed by the tool.

The CockpitCI architecture is also described in two versions, basic and advanced. The basic version is essentially a decision support tool which does not affect the operations of the CI; the advanced version is more ambitious since it includes additional automatic reaction capabilities.

Three characteristics have been identified as essential for a smooth acceptance of the CockpitCI tool by end-users:

- security,
- effectiveness,
- simplicity.

The security issue is discussed in a dedicated section. The basic configuration of the tool is characterized by a high level of intrinsic security and poses no threat to the CI operation since no automatic reaction mechanisms are present; it provides passive monitoring and operates as a decision support tool. The advanced configuration of the tool includes automatic reaction mechanisms and this makes the picture more complex in terms of security. Anyway a state-of-the-art approach to security and a balanced risk based approach should suffice to render acceptable automatic countermeasures which generally in presence of relevant risks tend to put the system in a safe-mode state and avoid potentially heavier consequences.

Regarding effectiveness, the CockpitCI tool promises to provide increased performance with respect to other solutions. The main winning points are as follows:

- inclusion of the cyber factor in the awareness picture;
- identification, in near real-time, of the CI functionalities impacted by cyber-attacks and assessment of the relevant degradation of CI delivered services;
- activation of strategies of containment of the possible consequences of cyber-attacks;
- leverage the ability of field equipment, in coordination with the central control level or autonomously, to counteract cyber-attacks by deploying preservation and shielding strategies

The CockpitCI tool is not simple, it is a sophisticated tool, yet it has been shown that the tool interface may be kept simple by hiding all the details of the implementation and provide a human interface at a higher level of abstraction.

This document cannot be considered a final and exhaustive document regarding system architecture. Significant tasks regarding automatic strategies have just begun and significant work regarding main system components is still underway, in accordance with the project timeplan. The analysis and refinement of the system architecture will therefore continue in the following months taking into account that significant feedback, updates and contributions will be provided by specific tasks addressing the main system components (IRP, DL and SMN) and currently running.

Finally, it is often stated that the CockpitCI project is a continuation and extension of the MICIE project, yet the CockpitCI project is in the opinion of the authors much more complex. The cyber factor and its inclusion in the global picture represent formidable research challenges and also the opening to automatic reactions at the central and local level represents a very challenging innovative objective.

8 References

[1] D5.1–“CockpitCI System requirements”, EU-FP7 CockpitCI project, http://www.cockpitCI.eu, May 2012.

[2] D3.1.1–“Requirements and Reference Architecture of the Analysis and Detection Layer-Preliminary”, EU-FP7 CockpitCI project, http://www.cockpitCI.eu, September 2012.

[3] SANS Institute InfoSec Reading Room, IDMEF – “Lingua Franca” for Security Incident Management, 2003.

[4] FP7 MICIE project, http://www.micie.eu

[5] D4.2-Secure Mediation Gateway Architecture, EU-FP7 MICIE project, http://www.micie.eu, Final Version.

[6] D4.1.1 - Online Integrated Risk Predictor and SCADA Adaptor Requirements and Design-Preliminary, EU-FP7 CockpitCI project, http://www.cockpitCI.eu,October 2012.

[7] Masera M., Fovino I., Vamanu B., “ICT aspects of power systems and their security”, JRC Scientific and Technical Reports, 2010.