FP7-SEC-2011-1 Project 285647

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

D6.1 – Validation Plan-Final

General information	
Submission date	31/12/2013
Dissemination level	Public
State	Final Version
Work package	WP6000-System Validation
Task	Task 6001 Validation plan and scenarios design and implementation
Delivery date	29/01/2014

Editors

Name	Organisation
Leonid Lev	IEC

Authors

Name	Organisation
L. Lev, D. Tanenbaum, L. Rozenblum, O. BenArush	IEC

Reviewers

Name	Organisation	Date
Roman Tania Ecaterina	TRANS	28/12/2013
Are Kvinnesland	Lyse	20/12/2013

Management Summary

This document provides the Validation Plan in line with the WP6000 task schedule.

ICSs (Industrial Control Systems) include supervisory control and data acquisition (SCADA) systems, distribution management system (DMS-SCADA), energy management control system (EMS-SCADA), distributed control systems (DCS), and other control system configurations such as Programmable Logic Controllers (PLC), normally used in industrial contexts such as utilities (electricity transmission, distribution and production, water supply and sewer processing, natural gas distribution), oil complexes or chemical processing, among others. SCADA systems control dispersed assets using centralized data acquisition and supervisory control. DMS and EMS are decisional control systems, generally used to optimise the performance of distribution and transmission energy network, DCS are generally used to control production systems within a local area such as a factory using supervisory and regulatory control. PLC generally used for discrete control for specific applications and generally provide regulatory control. These control systems are vital to the operation of critical infrastructures that are often highly interconnected and mutually dependent systems.

CockpitCI project intends to investigate a tool that could detect and react to cyber anomalies on SCADA and corporate network of a utility, to be demonstrated on a power distribution grid. During the WP6000 implementations the Validation system and methodology for CockpitCI tool validation designed and implemented. The results of the CockpitCI tool validation will be evaluated and recommendations for future CockpitCI tool implementation will be issued. The subject of this document is to design the Validation Plan that will integrate the validation of the overall concept including functionalities and performances and will include the requirements to the validation of the integrated CockpitCI tool. The CockpitCI tool validation process will start after all the CockpitCI components implemented in the different WPs testing will be completed. The Validation Plan is based on the Verification and Validation (V&V) process. Validation Plan includes the list of scenarios for CockpitCI verification and validation, scope of the CockpitCI tool Validation system and the methodology of the CockpitCI tool verification and validation. The validation system includes the CockpitCI tool, Hybrid Test Bed (HTB), Verification and Validation Scenarios, the tools for verification and validation process management and cyber-attacks simulation.

The HTB is a distributed environment that provides the parallel operation of the different user of the HTB. Customising to the CockpitCI project the HTB provides to the project partners resources for tool components development, test and integration; running different scenarios during CockpitCI tool validation; store validation results and return to the previous versions of scenarios.

Verification scenarios provide the cross reference of the tests and requirements as also the requirement management possibilities during the CockpitCI tool design, test and implementation. At the end of the verification process the CockpitCI tool will be tested to the entire stated requirements.

The CockpitCI tool validation scenarios implementation ensure that the tools' functions will be implemented as needed in its intended environment, including its operational behaviour, and user interface. The hardware and the software will be validated at the system integration level. CockpitCI tool validation will determine that a system will execute all the things it

should and will not do what it should not do. CockpitCI validation will be performed by an independent IEC team and will be performed in the validation system environment.

CockpitCI verification and validation Process will be managed by Quality Centre (QC) which is WEB based. Every partner will have WEB access to view the validation process and status.

The delivery D6.1 presents the verification and validation methodology for the CockpitCI project, validation system concept description and scope.

The delivery D6.1 "Validation Plan" includes the description of the validation system that includes: the Hybrid Test Bed (HTB), the verification procedures, the validation procedures and the traceability between CockpitCI requirements and verification and validation procedures realized by the Quality Center (QC) tool.

Table of contents

List of figures

List of tables

1 Introduction

1.1 Context

CockpitCI project intends to investigate a tool that could detect and react to cyber anomalies on SCADA and corporate network of a utility, to be demonstrated on a power distribution grid. During the WP6000 implementations the Validation system and methodology for CockpitCI tool validation were designed and implemented. The results of the CockpitCI tool validation will be evaluated and recommendations for future CockpitCI tool implementation will be issued. The subject of this document is to design the Validation Plan that integrates the validation of the overall concept including functionalities and performances and will includes the requirements to the validation of the integrated CockpitCI tool. The CockpitCI tool validation process will start after all the CockpitCI components implemented in the different WPs testing will be completed. The Validation Plan is based on the Verification and Validation (V&V) process. Validation Plan includes the list of scenarios for CockpitCI verification and validation, scope of the CockpitCI tool Validation system and the methodology of the CockpitCI tool verification and validation. The validation system includes the CockpitCI tool, Hybrid Test Bed (HTB), Verification and Validation Scenarios, the tools for verification and validation process management and cyber-attacks simulation.

The HTB is a distributed environment that provides the parallel operation of the different users of the HTB. Customising to the CockpitCI project the HTB provides to the project partners resources for tool components development, test and integration; running different scenarios during CockpitCI tool validation; store validation results and return to the previous versions of scenarios.

Verification scenarios provide the cross reference off the tests and requirements as also the requirement management possibilities during the CockpitCI tool design, test and implementation. At the end of the verification process the CockpitCI tool will be tested to the entire stated requirements.

The CockpitCI tool validation scenarios implementation will ensure that the tools' functions will be implemented as needed in its intended environment, including its operational behaviour, and user interface. The hardware and the software will be validated at the system integration level. CockpitCI tool validation will determine that a system will execute all the things it should and will not do what it should not do. CockpitCI validation will be performed by an independent IEC team and will be performed in the validation system environment.

CockpitCI verification and validation Process is managed by WEB based Quality Centre (QC). Every partner has WEB access to view the validation process and status.

The delivery D6.1 presents the verification and validation methodology for the CockpitCI project, validation system concept description that includes as follows: the Hybrid Test Bed (HTB), the verification procedures, the validation procedures and the traceability between CockpitCI requirements and verification and validation procedures realized by the Quality Centre (QC) tool.

1.2 Objectives

The objective of WP6000 is to validate the technology of the CockpitCI system. The CockpitCI system will be validated on real historical (recorded) SCADA data. After that the

CockpitCI will be evaluated using the Validation system that includes: the HTB (Hybrid Test Bed) based on real but not the operational SCADA systems, operation systems, communication and field equipment as also the tools for control of the data traffic, interfaces and possibilities to connect the partners to the HTB, verification and validation scenarios.

The Validation Plan design is based on the CockpitCI system architecture design (WP5002), Reference Scenarios provided by IEC to WP2002 and HTB customization for CockpitCI Validation.

The Validation Plan is developed before the validation process of the CockpitCI will start. The Validation Plan integrates the validation of the overall concept including functionalities and performances and l includes the requirements to the validation of all the products implemented in different WPs. The Validation Plan is based on the Verification and Validation (V&V) process that will be provided for every subsystem and product under responsibility of the corresponding WP leader. Validation Plan includes the scenarios for CockpitCI validation. Those scenarios are coordinated with the project integrator and all WP leaders.

The Validation process definition is based on the CockpitCI architecture, validation plan and operational scenarios that can be used for development of various types of simulators for the validation of the CockpitCI.

The WP6000 consists of the following tasks (see DoW):

- Task 6001: Validation plan and scenarios design and implementation will be developed before the validation process of the CockpitCI will start. The Validation Plan will integrate the validation of the overall concept including functionalities and performances. The Validation Plan will be based on the Verification and Validation (V&V) process and will include the scenarios for CockpitCI validation.
- Task 6002: Aggregation of the CockpitCI system with the Validation system that will include: HTB (Hybrid Test Bench), verification and validation scenarios and designed CockpitCI tool. The main purpose of the HTB is to simulate the real Critical Infrastructure (CI), validation scenarios and simulation tools. During the implementation of the Task 6002 the HTB will be integrated with the CockpitCI tool and verified according to the requirement specification.
- Task 6003: CockpitCI Validation phase will cover all the issues of the project. The Validation system environment will be based on the real equipment installed in the non-operating premises. This equipment will simulate the real scenarios to validate CockpitCI system. During this step, the real but not the operational SCADA data will be checked. In this step, simulations will be used since such testing cannot be done on an operational SCADA system. The simulated system will include all the HW, SW, HMI, Control Centre, communication devices and connections typical to a real system. All the data security aspects, operational scenarios and simulations could be validated at this stage

1.3 Document Structure

The chapter of the document respectively deals with:

- Chapter 2 describes the CockpitCI validation concept including Verification and Validation (V&V) concept, aggregation of the reference scenarios models and validation scenarios concept, simulation models

concept, validation process implementation overview and validation process management.

- Chapter 3 describes a Validation system scope including overview of Validation System configuration, CockpitCI configuration, Hybrid Test Bed (HTB) configuration and customization for the CockpitCI project, Verification scenarios, Validation scenarios scope and Validation Process Results Evaluation concept.
- Chapter 4 deals with conclusions of validation plan development and implementation
- Appendices describe the HTB test plan and requirements traceability.

Only public documents have been considered, being properly referred along this document.

1.4 References

1. D2.2- Reference Scenario – SCADA system of Power grid and corporate network under cyber-attacks – Preliminary report
2. D5.1 – CockpitCI System requirements
3. D5.3.1- Secure Mediation network design and specification – Preliminary version.
4. CockpitCI Consortium, Cybersecurity on SCADA: risk prediction, analysis and reaction tools for Critical Infrastructures, Project Proposal, PART B 2011.
5. Ralph R. "Young the Requirements Engineering handbook" Artech House, 2004
6. James N. Martin "System Engineering Guidebook" CRC Press 1997

1.5 Glossary

Not Applicable

1.6 Acronym and symbols

Acronym or symbols	Explanation
AAA	Authentication, Authorization, Accounting
ACL	Access Control List
ARP	Address Resolution Protocol
CERT	Computer Emergency Response Team
CIA	Confidentiality, Integrity, and Availability
COTS	Commercial off the Shelf
DBMS	Database Management Systems
DCS	Distributed Control System

DDoS	Distributed Denial of Service
DDoS	Distributed Denial of Service
DIDS	Distributed IDS
DMS	Distribution Management Systems
DMZ	Demilitarized Zone
DNS	Domain Name System
DoS	Denial of Service
EMS	Energy management Systems
HIDS	Host Intrusion Detection Systems
HMI	Human-Machine Interaction
HTB	Hybrid Test Bed
FW	Firewall
ICMP	Internet Control Message Protocol
ICT	Information and Communication Technologies
IDMEF	Intrusion Detection Message Exchange Format
IDS	Intrusion Detection System
IP	Internet Protocol
IRP	Integrated Risk Prediction
LAN	Local Area Network
MITM	Man-In-The Middle
NIDS	Network Intrusion Detection Systems
NIST	National Institute of Standards and Technology
OLE	Object Linking and Embedding
OPC	OLE for Process Control
OSI	Open Systems Interconnect
PLC	Programmable Logic Controller
QoS	Quality of Service
RDBMS	Relational Database Management System
RTU	Remote Terminal Unit
SCADA	Supervisory Control and Data Acquisition
STP	Spanning Tree Protocol
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
V&V	Verification and Validation
VPN	Virtual Private Networking
WAN	Wide Area Network

2 CockpitCI Validation Concept

2.1 Verification and Validation

Validation of the R&D product cannot be performed on the real operational infrastructures so different types of simulations are used for R&D product validation. The validation process split into verification and a validation steps.

The objective of the verification process is to ensure conformance of the implemented product and processes to all initial and derived requirements and that the planned development process has been accurately followed. Verification is the tasks, actions and activities performed to evaluate progress and effectiveness of the evolving system solutions (people, products and process) and to measure compliance with requirements. Analysis (including simulation, validation, test and inspection) are verification approaches used to evaluate risk, people, product and process capabilities, compliance with requirements and proof of concept.

The objective of the validation process is to ensure that the product functions have been implemented as needed in its intended environment, including its operational behaviour, maintenance, training and user interface.

The hardware and software are validated at the system integration level. This is a step beyond the software and hardware verification processes. Validation is interpreted as the validation of the design to the requirements, utilizing mission-type hardware to the extent possible. Validation is a determination that a system does all the things it should and does not do what it should not do. Validation may be performed in the operational environment or a simulated operational environment.

Successful verification and validation confirms that the development process has provided a system consistent with customer expectations. Additionally verification provides safeguards, so the development program does not backtrack. It also ensures a development product and processes that meet the applicable functional, behavioural, timing, weight, power, performance, configuration, reliability, and maintainability requirements.

Real equipment is a part of the Validation System and is installed at the IEC premises. This equipment is configured as the portion of real infrastructures. In order to adequately account for the users and operators of the system, a wide variety of scenarios is defined.

Validation System includes as follows: a Hybrid Test Bed (HTB), CockpitCI tool, partners labs resources and cyber-attacks simulations.

A hybrid is the combination of two or more different disciplines, aimed at achieving a particular objective or goal. For instance, two types of computers, analogue & digital, were the analogue computer is used to simulate the real control process including the solution of differential equations, while the digital computer served for control and logical operations and virtual processing. As an integrated system, the two computers make up for the shortcomings inherent in each one of them.

By the same principle, we use the name "hybrid" for explaining the combination of the real physical equipment installed at IEC premises with the real Reference scenarios and real working procedures. This hybrid approach allows us to combine the effects of real

environmental factors with the models and simulations that complete the overall environment effect.

The Reference scenarios are used to build tasks and job analyses for the operators and users and to test designs and procedures. Since these scenarios are written from the point of view of the users and operators, they can be excellent vehicles for soliciting feedback during user reviews. Scenarios can be simply represented as written descriptions or storyboard sequences and therefore, they can be used in early stages of system development. The detailed inner workings of the hardware and software do not need to be defined because such details are irrelevant from the user's point of view. The Reference scenarios of the Validation System are designed, from the user's point of view and detail events of the system mission, including identification of mission phases, mission time scale, and events external to (and their interactions with) the system.

The Working procedures define the operator's decision making scenario during different events (including cyber-attacks) that could happen in real environment.

The validation procedures are based on the Reference scenarios and working scenarios implemented in the Validation system.

In order to carry out the validation task as described above, IEC uses the HP "Quality Centre", a web-based system for automated software quality testing across a wide range of application environments. It is designed to automate activities, including requirements, test and defect. The Validation system implemented at the IEC premises. CockpitCI Verification & Validation reference model is presented in Fig.1.

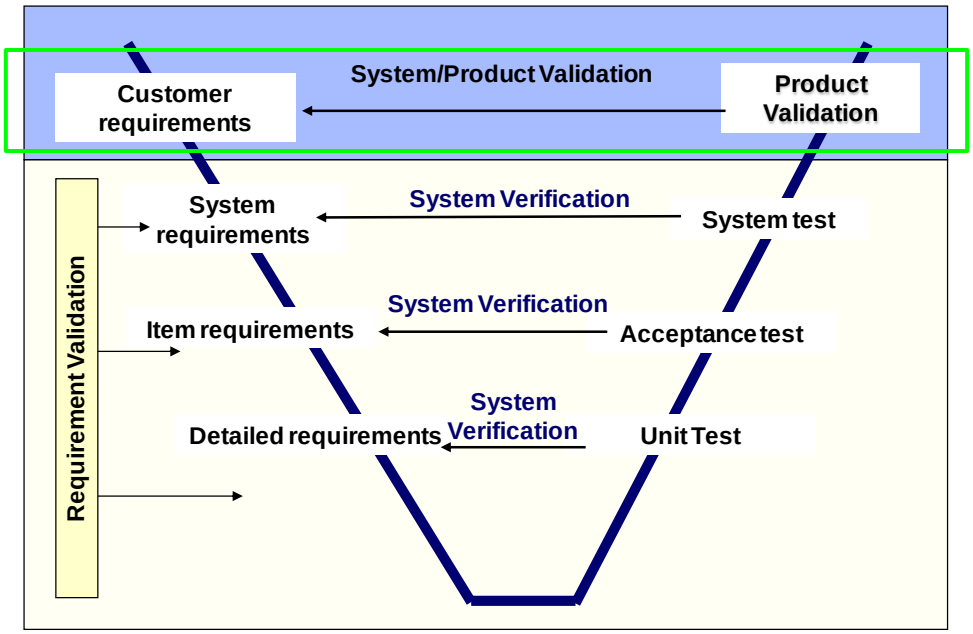


Figure 1: CockpitCI V&V reference model

All the system components will be tested during execution and integration of CockpitCI tool as follows:

- The integration of all the elements of the CockpitCI system, namely the Detection Tools, the Integrated Risk Prediction tool and the Secure Mediation Network will be implemented in WP5000,
- Verified CockpitCI platform will be validated during WP6, in accordance with the requirements provided in the WP5.

2.2 CockpitCI tool Verification process

The objective of the CockpitCI tool verification process is to ensure conformance of the implemented CockpitCI tool to all the requirements described in the deliverable D5.1 "CockpitCI System requirements" and that the planned CockpitCI tool development process has been accurately followed. Verification tasks, actions and activities performed to evaluate the CockpitCI solutions with requirements are described in the Appendix of the deliverable D6.1.

Verification process in the CockpitCI project is based on Quality Center (QC) tool that is the part of the Validation System described in the current document. The CockpitCI requirements are added to the QC database. The Test Plan designed and crossed to the correspondent requirements. During the last state of verification design the test cases will be designed and crossed to the Test Plan and requirements.

This QC provides the cross reference off the tests and requirements as also the requirements management possibilities during the CockpitCI tool design, test and implementation. At the end of the verification process the CockpitCI tool will be tested to the entire stated requirements.

2.3 CockpitCI tool Validation process

The objective of the CockpitCI tool validation process is to ensure that the tools' functions have been implemented as needed in its intended environment, including its operational behaviour, and user interface.

The hardware and software will be validated at the system integration level. This is a step beyond the software and hardware verification processes. CockpitCI tool validation will determine that a system will execute all the things it should and will not do what it should not do. CockpitCI tool validation will be performed by an independent IEC team and will be performed in the validation system environment.

CockpitCI tool successful verification and validation will confirm that the development process will be provided a system consistent with project expectations. Additionally verification will provide safeguards, so the development program will not backtrack and CockpitCI will meet the applicable functional, behavioural, performance and configuration requirements. The CockpitCI validation process is presented in Fig. 2. The validation process will be implemented by several steps:

Step1 "Model" – during this step validation model that aggregates References Scenarios, Working Procedures and CIs' description will be developed and implemented. This model describes the behaviour of CIs in different situations and conditions.

Step2 "Data" – during this step the historical data contributed to model designers. This data is an input to all simulation scenarios implemented during the project.

Step3 "HTB design and implementation" – during this step HTB is customized to the CockpitCI project. The customization includes design, procurement of the necessary equipment, licenses, SW and communication; aggregation of the components, installation and HTB validation. HTB is customized in order to aggregate the HTB and CockpitCI tool on the level of bidirectional protocols (like OPC, MTOSI, etc.) and models implemented in the CockpitCI tool.

During the Task 6001 the first three steps are implemented

Step4 "HTB and CockpitCI tool Integration" will be implemented during the Task 6002 and the Task 6003. This step will finish the CockpitCI tool tests by the platform designer. During this step the CockpitCI tool will be installed, will be run and will be integrated with the HTB equipment, scenarios and data. The Step4 will be followed by the CockpitCI tool validation and evaluation.

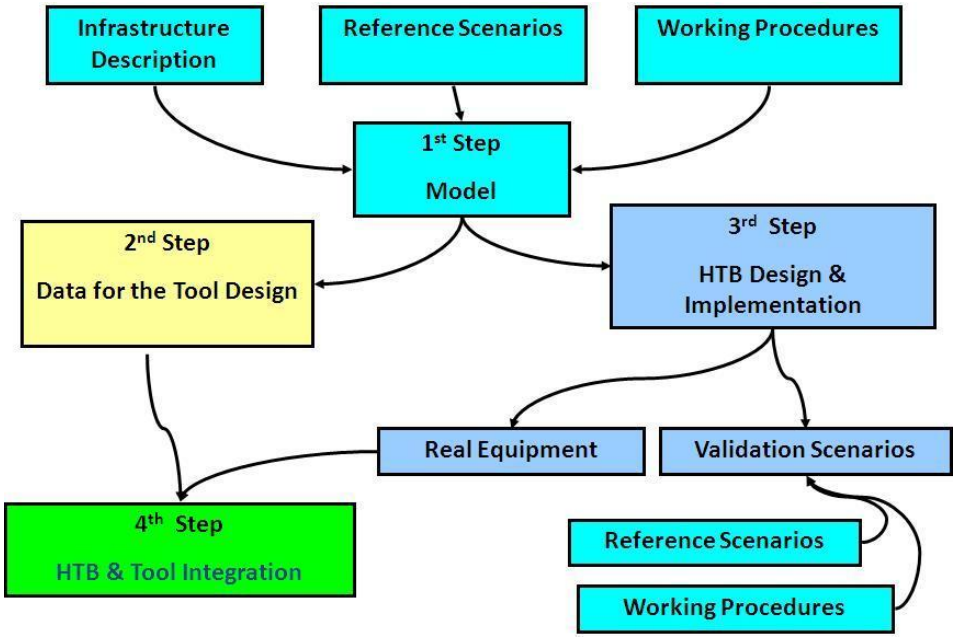


Figure 2: Validation Process concept

Matching the CockpitCI validation concept the Electric CI (ECI) is represented by the real non-operational equipment installed in IEC, Roma3 and Coimbra University, and simulation of the Electric CI dynamic model and includes the components as follows: the electric elements, the RTUs that enable command and control over the elements and SCADA HMI.

The operator of the HTB plays the role of the Electric grid dispatcher. The HTB contains real equipment and simulated equipment. The operator dol not distinguish between those components.

The ECI simulator simulates the following electrical grid components:

- two primarily transformer stations,
- sections of 2 MV feeders,
- HMI SCADA for working processes execution.

HMI (Human Machine Interface) is a set of high level commands (the terms are familiar to the dispatcher), as defined in the following sections. (E.g., "power line section"). The commands are sent by SCADA to simulator and are interpreted by it to update elements states and values matching the real equipment.

2.4 CockpitCI tool Verification and Validation (V&V) Process Management

CockpitCI Validation Process is managed by Quality Center (QC) which is WEB based. Every partner has WEB access to view the validation process and status.

The V&V management includes the following capabilities:

- Requirements management,
- Requirements traceability,
- Test plan design,
- Verification scenarios design and implementation,
- Validation scenarios design and implementation.

V&V management examples are presented in the Appendices as follows:

- The test plan, requirement management and traceability tables derived from the Quality Center (QC) tool,
- The procedures presented by flowcharts derived from the Visio process tool.

IEC uses Visio process tool for complex systems and test procedures design (Smart grid concept design, Homeland security system, ENERsip test procedures). Visio process provide object oriented design diagrams which could be converted to the Excel tables and then automatically converted to the requirements or test procedures in the QC tool. After conversion to the QC tool the process of requirement and test management is implemented by the QC standard procedures.

3 Validation System Scope

3.1 Validation System Configuration

Real Equipment is a part of the Validation System and is installed at the IEC premises. This equipment is configured as the portion of real infrastructures. In order to adequately account for the users and operators of the system, a wide variety of scenarios is defined.

In order to carry out the validation task as described above, IEC uses the HP "Quality Centre", a web-based system for automated software quality testing across a wide range of application environments. It is designed to automate activities, including requirements, test and defect.

The CockpitCI validation environment includes the components as follows:

- Hybrid Test Bed (HTB)
- Validation and verification scenarios
- Quality Center (QC)
- Cyber Attacks scenarios

The scenarios preliminary list described in the sections 3.5 and 3.6. The Validation System Concept is presented in Fig.3.

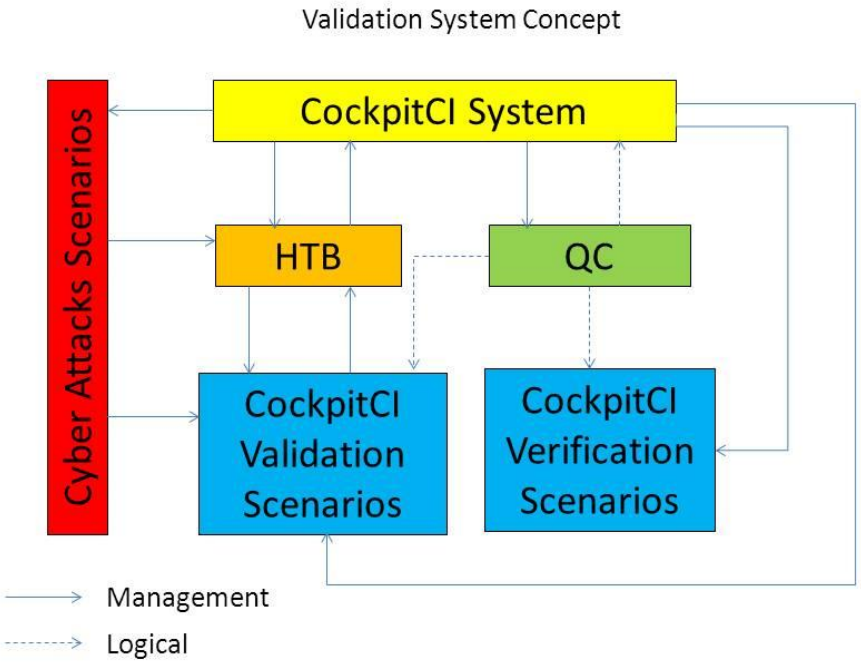


Figure 3: Validation System Concept.

3.2 CockpitCI Generic Configuration

The CockpitCI tool configuration described in the delivery D3.1.2 "Requirements and Reference Architecture of the Analysis and Detection Layer" and presented in Figure 4. The generic architecture is based on a distributed infrastructure that aggregates several probing and monitoring points, working together on close coordination to provide the surveillance capabilities for the security platform. The functional criterion for deploying those security probes (or sensors) divides the SCADA infrastructure on three different security zones, as follows:

IT Network

This is the organization's IT Network. While this network isn't part of the SCADA system, it may host SCADA components, like Human-Machine Interfaces (HMI) consoles. Also, historical evidence has shown that several successful attacks have found its way to the critical SCADA components through this level of the networking infrastructure.

Operations Network

This network hosts the main SCADA components, such as Master Stations, Database Management Systems (DBMS) servers or HMI Consoles.

Field Network

This network hosts the field devices, like Remote Terminal Unit (RTUs), and process sensors. This multi-zone topology provides a contextual approach to the problem of probe placement that takes into account the existence of different network scopes, which can be easily segmented and separated by a well-defined perimeter. It has two purposes: first, to separate different infrastructure contexts for which different detection, correlation/Inference and reaction strategies might apply; second, to provide well-defined security perimeters between each zone, which are critical to provide mediation mechanisms which may inspect and control information flows between each one. The CockpitCI tool configuration is detail described in the project documentation.

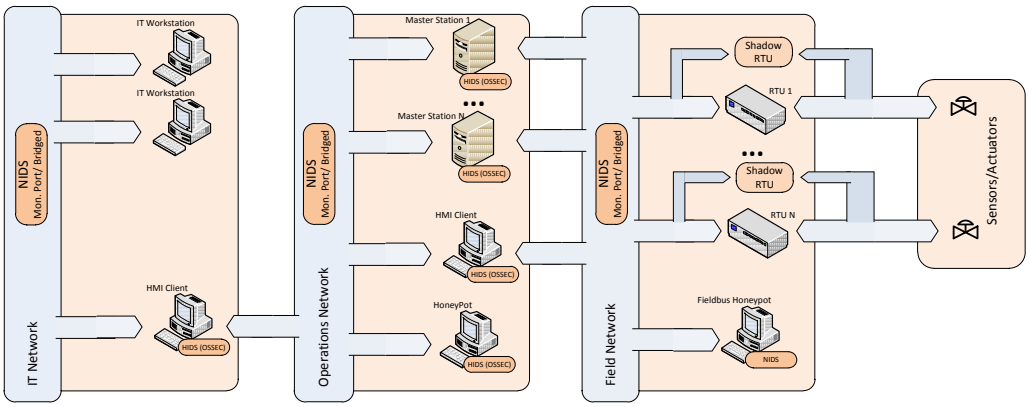


Figure 4: CockpitCI Platform generic configurations

3.3 Hybrid Test Bed

The HTB is a distributed environment that provides the parallel operation of the different users of the HTB. The HTB, customised to the CockpitCI project, provides to the partners resources for tool components development, test and integration; running different scenarios during CockpitCI tool validation; store validation results and return to the previous versions of scenarios. The Hybrid Test Bed provides the CockpitCI developers the following capabilities:

- Simulate operation scenarios (electrical grid and telecom) based on real SCADA and Network Management System (NMS), physical components of electrical and telecom infrastructure and elements that simulates electrical and telecom infrastructure,
- Collect and analyse real network traffic of heterogeneous networks (electrical grid, telecom network, SCADA),
- Test models and components for cyber-attack detection and identification,
- Test models and components for mitigation of cyber-attack influence on critical infrastructure,
- Test effectiveness of countermeasure's plans,
- Test effectiveness of automatic reaction logics,
- Test CockpitCI system functionality,
- Define every partner as a user with a predefined access level.

The HTB capabilities matching the CockpitCI tool are as follows:

- Possibility of the real infrastructure modelling.
- Possibility to record and to analyse real network traffic in every part of the network.
- Easy installation of new components for research and simulation purposes.
- Automatic procedure for operational process simulation.
- Automatic procedure for logs collection and storage.
- Remote access to test environment.
- Simulate separate logical test environments.
- Save logical test environments for reuse in future.

- Functionality and agility of CI test-environment.

HTB includes the components as follows:

- Electrical and telecom equipment,
- Virtual machine infrastructure,
- Test and requirement environment management infrastructure (QC and Visio process tools),
- Network-flow management infrastructure,
- SCADA management system,
- Telecom management system,
- Electrical infrastructure simulator,
- Elements of communication network infrastructure (SDH, Cellular, and VHF).

CockpitCI Validation system includes CI configuration as follows:

- SCADA with RTU's and PLCs that are installed for ECI (Electrical CI) simulation (e.g. swithers, transformers, feeders),
- Communication backbone based on transmission elements and F.O. cables,
- ECI simulation presents a portion of the power distribution system and its main services. ECI provides the possibility to manage the power flow from substations to MV/LV transformers,
- ICTCI (Information and Communication technologies CI) presents by the RTU's that helps ECI's operator to reconfigure the electrical grid remotely from Control Centre. Thus its main service is to ensure that those RTU's work properly,
- CCIs' (Communication CI) main service is to provide communication links between ICTCI elements. (E.g. computers, PLC and RTU's).

The HTB includes electrical grid RTU's that enable the supervisor to receive alarms, isolate the fault location and to restore power. All actions are done by open and close switches. The user in this scenario uses SCADA applications based on WIZCON or Cimplicity software that enable him to open/close switches as also to monitor simulated voltage and current measurements based on historical data.. The HTB concept view is presented in Fig. 5.

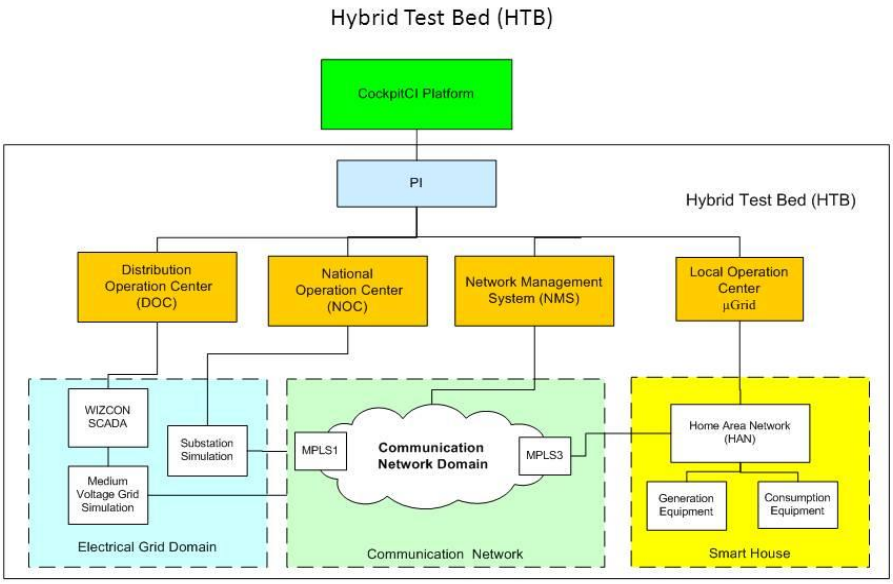


Figure 5: Hybrid Test Bed view

Following we describe the main components of HTB. The key element of HTB is the network-flow management infrastructure. Every physical and logical element of CI connected to the network-flow management infrastructure that includes the following components:

- Content Inspection Director (CID) is a core element of network-flow management infrastructure. CID manages logically defined network-flow redirection,
- Components for cyber-attack detection and identification,
- Components for mitigation of cyber-attack influence on critical infrastructure,
- Network-flow collectors and analysers,
- User access to the HTB components (servers, work stations, SCADA applications, etc.) managed by SSL (Secure Sockets Layer) VPN appliances,
- The components of the test-environment installed on remote sites of CockpitCI partners and connected to the HTB through VPN (Virtual private Network) channels based on FW-FW IPSEC (Internet Protocol Security) VPN.

CockpitCI HTB main components are presented in Fig.6.

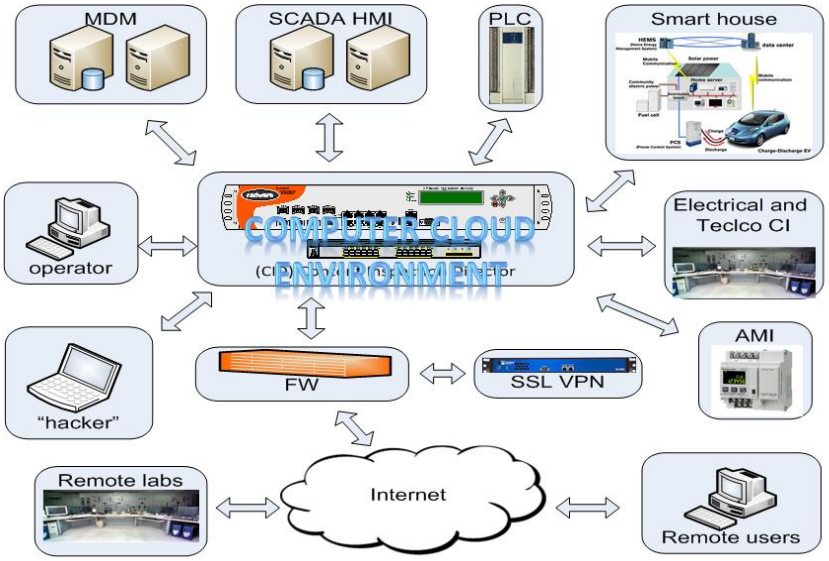


Figure 6: CockpitCI HTB main components

During the HTB customization for the CockpitCI project implementation the following elements were added to the basic configuration: remote labs, hacker attacks server, CI simulators.
HTB was customised to the CockpitCI configuration described in the Deliverable D3.1 and strictly summarized in the section 3.2 of this document. The main customization efforts were as follows:

- Aggregation of remote labs from Roma3 and Coimbra universities to the CockpitCI Validation system,
- Connection of the ENEA and Itrust partners,
- Implementation of the bidirectional remote access to all recourses of the CockpitCI Validation system,
- CockpitCI tool and HTB aggregation in the CockpitCI Validation system,
- Development of the verification and validation scenarios for CockpitCI tool verification and validation,
- Definition of the servers resource according to the CockpitCI structure: IT (the company level), OP (SCADA systems level) and Field (RTUs, PLCs and other devices),
- On the IT network the following systems are installed: WEB Server, Correlators, Management Server, NIDS, Honeypots and others.

- On the OP network the following systems are installed: HMI SCADA, HMI consoles, Management Server, CockpitCI system, Security GWs for connection of different CIs to the CockpitCI system, NIDS, Honeypots.

- On the Field network the following systems and equipment are installed: the Virtual Machines (VM) as follows: Field Simulators for simulation of different infrastructures, PLCs and RTUs, HIDSs and Honeypots,

- Installation of different operational systems (Windows XP, Windows7, Windows2008 and so on).

Aggregation of the Roma3 and UC labs as also as connection of the resources of the other partners to the HTB was implemented by several stages as follows:

- IEC l sent to the partners the questioner tables and procedures for connection to the HTB,

- Two labs in Roma3 and UC universities were connected to HTB as also the ENEA and iTrust partners,

- The consortium will decide the level access for every partner

- The other partners will be connected to the HTB.

HTB customized configuration is presented in the Fig. 7.

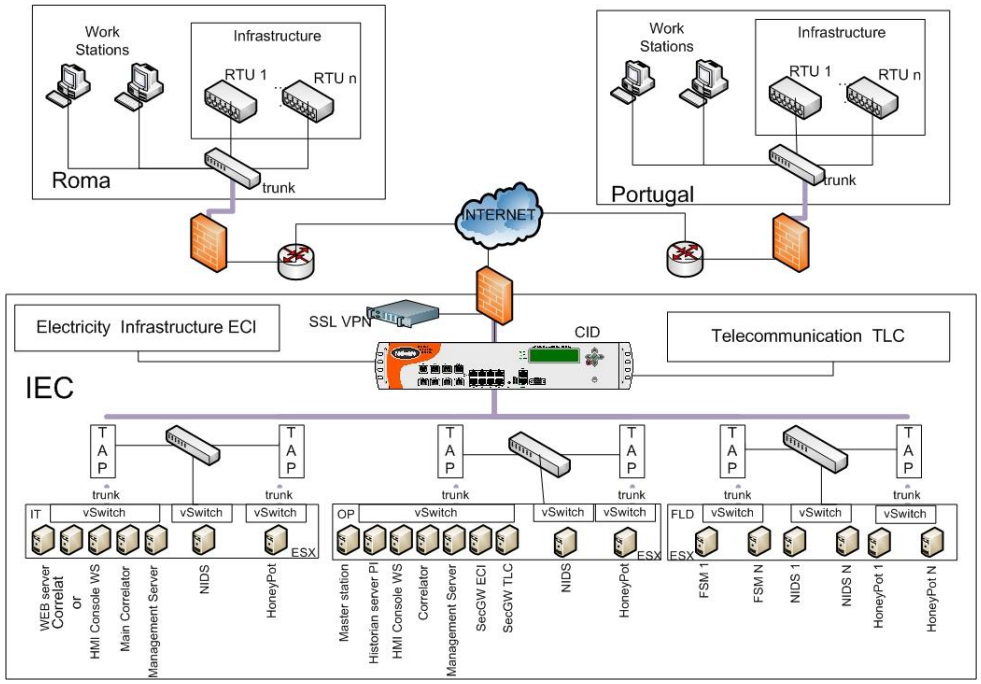


Figure 7: CockpitCI customized HTB configuration

3.4 Simulation Models Concept

CI simulation concept for HTB is based on the several mane principals as follows:

- No real operation CI are used
- CI simulation are performed by the several levels as follows:
    - CI physical simulation model,
    - Field equipment simulation model,
    - Communication simulation model,
    - HMI simulation model.

Level 1 CI physical simulation

Level 1 l represents different CIs and interconnections between CIs. CI physical simulation level performed by:

- Real non-operational physical segments: fiber optic cables, electrical LV customer equipment, electric LV producer equipment like photovoltaic panels or wind mills,
- PLCs that represent different CI segments and parameters for every segment. Those parameters are transferred to the 2nd level (1 port for every segment) as follows:

a. Primary Substation:
    1. Segments: transformers, CBs,
    2. Parameters: current, voltage, load, transformer.

b. Medium Voltage (22KV):
    1. Segments: Feeder segment (from switch to next switch), switch, transformer 22KV/0.4KV,
    2. Parameters: current, impedance and voltage for every segment of the feeder for every configuration of the feeder during FISR (Fault Isolation and Restoration) procedure execution.

c. Low Voltage
    1. Segments: homes,
    2. Parameters: current, impedance and voltage for every segment.

d. Communication
    1. Fiber optic cables,
    2. Radio equipment,
    3. Wireless communication equipment like Wi-Fi, Zigbee.

CI physical simulation level could not be damaged by cyber-attacks. CI physical simulation level modeled by real equipment or by PLCs that use real data as inputs and simulate measurements and events as outputs.

Level 2 is a Field Equipment Simulation Model Level that represented by different PLCs, RTUs, sensors and other equipment This equipment could be IP based (all modem equipment IP based) or not. The Level 2 equipment could be damaged by cyber-attacks and has different industrial protocols like: Modbus, Profibus, MPLS and so on. Field Equipment Simulation Level uses measurements and events from CI physical simulation as inputs. The outputs of the Field equipment simulation model are data that transferred to the HMI Simulation Model via the Communication Simulation Model.

Level 3 is a Communication Simulation Model that represented by routers, MUXs, gateways which are IP based. This equipment is very sensitive to cyber-attacks. Communication Simulation Model transfers data from the Field Equipment Simulation Level to the HMI Simulation Model.

Level 4 is a HMI Simulation Model that is presented by different industrial SCADA HMI like: Cimplicity, WIZCON, and PC IM. This level is the most sensitive ICSs' level for cyber-attacks. All the long history of the industrial SCADA HMI were not protected like the IT systems because those systems were not open to the WEB but last years the situation changed dramatically and most of the ICSs use WEB for communication. The main protocols used for connection of HMI Simulation Model are: OPC, ICCP, MTOSI and others. PI system used for integration of different HMI SCADA and connection to HTB external systems. The PI System is the industry standard in enterprise infrastructure for management of real-time data and events. The overall concept of simulation models concept is presented in Fig.8.

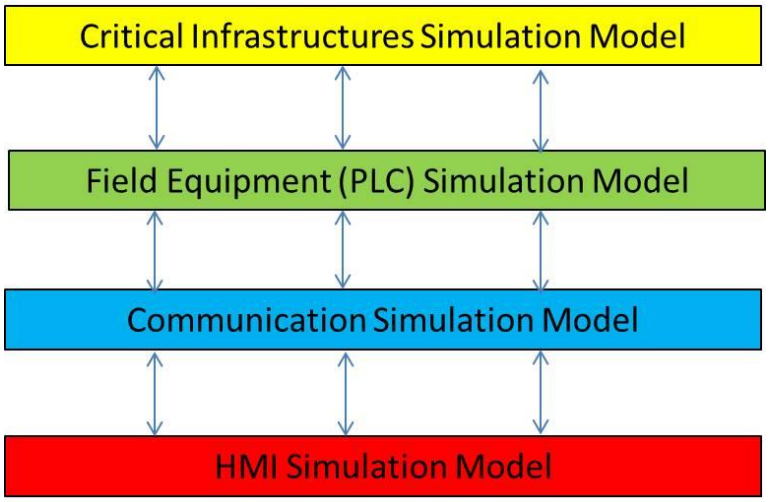


Figure 8: Simulation Model concept

3.4.1 ECI (Electrical Critical Infrastructure) simulation scenario

ECI simulation scenario includes: simulation of the energy transportation including substations, Medium Voltage (MV) electrical grid and Low Voltage electrical grid presented by Smart Home with generation and consumption capabilities. ECI simulation includes three CI simulation levels as follows: Critical Infrastructures Simulation model, Field Equipment Simulation Model and HMI Simulation Model.

ECI simulation provides the capabilities as follows:

- Flexibility in design and implementation of different ECI configurations.
- Calculate performance indicators given various scenarios (especially fault scenarios), not including cyber-attacks on the SCADA and RTU's.
- Possibility of implementation of cyber-attacks to the Failed Equipment, communication and HMI simulation models.

- Investigating possible effects on the system under cyber-attacks.
- Investigating the effects of CockpitCI tool in the simulation environment.
- Integrate real electric devices in the simulation environment.

The ECI simulation configuration presented in Fig. 10 is based on the HTB concept presented in Fig.5 and Simulation Model concept presented in Fig.9 and described below.

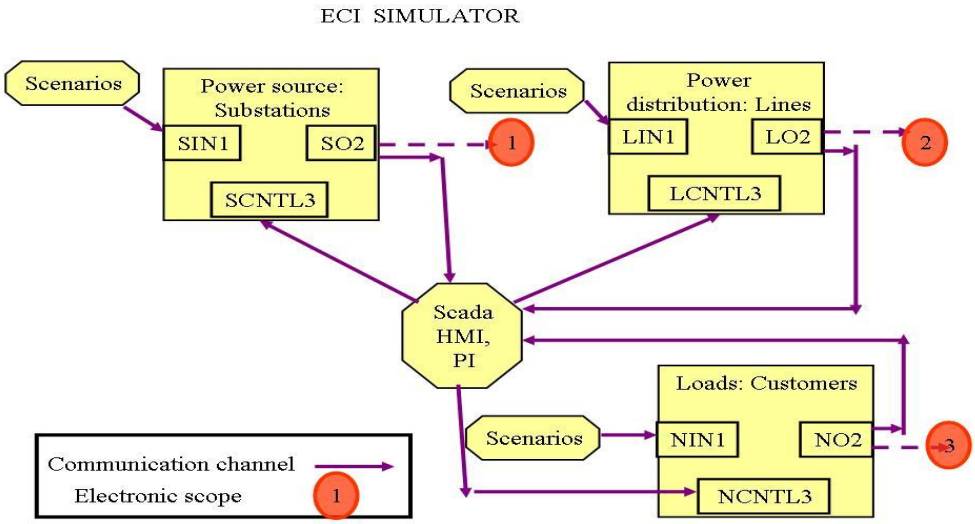


Figure 9: ECI Simulation Model Configuration.

3.4.1.1 Substation simulation

Substation simulation or Power source implemented by PLCs aggregated in two functional types:

- The PLCs of the first functional type simulate the electrical grid elements like: transformers, circuit break (CB), bus lines and so on. The purpose of this scenario is to simulate substation measurements 24 hours a day. The input data is the measurement results from the real substation elements. This type of PLCs does not be accessible for cyber-attacks. Those PLCs have input ports (SIN) for changing electrical parameters of the substation, output ports (SO) for transfer simulated measurements and events to the field equipment and for connection the HMI (SCNTL) for management of the simulation process by external HMI.

- PLCs of the second functional type simulate the field equipment that includes PLCs that simulates the SCADA installed in substation. PLCs inputs connected to the outputs of the PLCs of the first type and outputs connected to the SCADA HMI. Those PLCs are accessible for the cyber-attacks.

- The SCADA HMI simulates the National Operation Centre (NOC) operation and is accessible for the cyber-attacks also.

3.4.1.2 Medium Voltage Simulation Scenario

Simulation of the ECI Medium Voltage grid is an aggregation of the electrical grid elements, Field equipment and HMI SCADA.

There are two functional types of the PLCs:

- The PLCs of the first functional type simulate the electrical grid elements like: transformers, cables and switchers. The purpose of this scenario is to calculate performance indicators related to Fault Isolation and Service Restoration process. This type of PLCs does not be accessible for cyber-attacks.

- The PLCs of the second functional type simulate the field equipment that include PLCs that simulate the secondary substations command and control process. These PLCs also have inputs connected to the outputs of the PLCs of the first type and outputs connected to the SCADA HMI. The purpose of this scenario is to simulate the process of health check of the grid RTU's from the control center. The effect of fault in RTU on the grid operation can be demonstrated. Those PLCs are accessible for the cyber-attacks.

- The SCADA HMI simulates the Distribution Operation Center (DOC) operation.

The PLCs' configuration that simulates the Medium Voltage presented in Fig. 10.

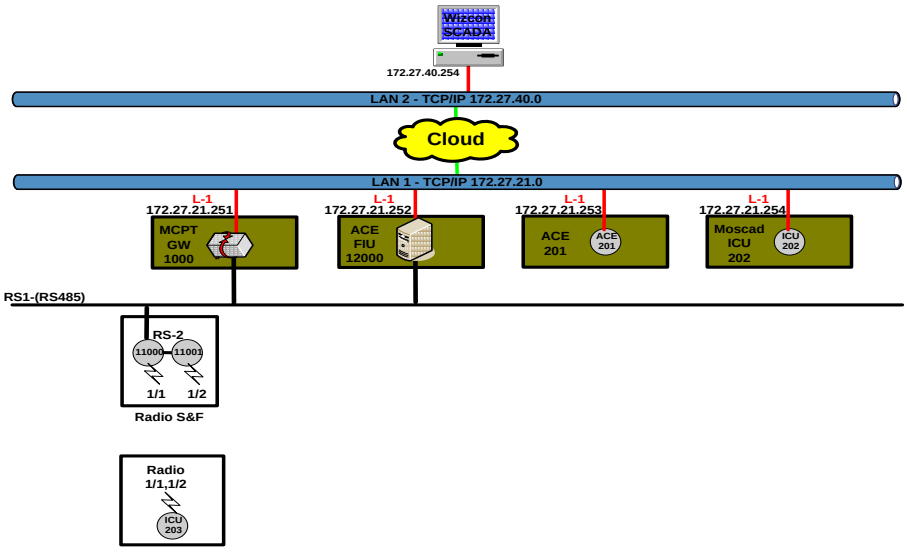


Figure 10: Medium Voltage Field Equipment simulation

3.4.1.3 Smart Home Simulation scenario

Smart Home simulation scenario represents the typical season and daily behaviour of Low Voltage consumption and distribution. This modelling is based on typical multi tariff and typical load profiles of the different house appliances.

There are two types of PLCs simulating the Smart Home:

- The first type simulates the typical consumption behavior and sends switch on/off commands to the home appliances. These PLCs perform the typical loads of the home appliances also.

- The second type of PLCs is the real Zigbee based elements for remote smart house managing like: plugs for remote command and control of home appliances, HAN (Home Area Network) GW, temperature and humidity sensors, plugs for local generation measurements and so on.

Smart Home simulation scenario is presented in Fig. 11.

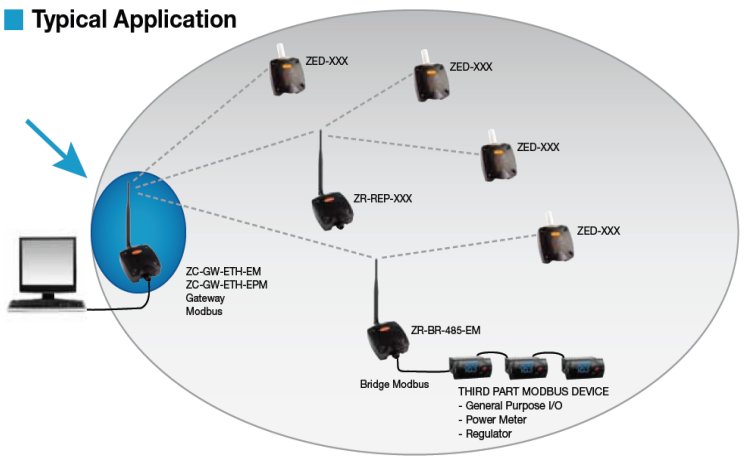


Figure 11: Smart Home simulation configuration

3.4.2 Communication CI Simulation

Communication CI (CCI) simulation is based on real fibber optic and MPLS non-operational systems and includes equipment as follows:

- Fiber optic network equipment that includes: switchers like BGs, XDM connected in ring configuration,

- Network Management System (NMS) that provides remote management of the fiber optic equipment,

- MPLS switches,

- DVR and video cameras connected to the MPLS switchers,
- Network management system (NMS).

The HTB communication network is based on several elements presented in the Fig.12. Some of the elements are real equipment and some of them are simulated by NMS. The picture presented in the figure is real time display of the NMS.
The digital transmission equipment that is used by HTB is the following:

- SDH (Synchronous Digital Hierarchy) that supplies 3 major services, it's also defined a multiplexing structure whereby an STM-N (Synchronous Transport Module level N) or STS-N (Synchronous Transport Signal level N) aggregated:

a. 64K channel supports one telephone line or RS 232, RS 485, etc.
b. 2M (E1 protocol) channel – supports up to 30 telephone lines.
c. Ethernet channel – supports 10/100/1000M band width for all computer services used by most of the companies.

- BG is SDH/STM technology equipment supporting 4 channels,
- XDM is SDH/STM technology equipment supporting 16 channels.

MPLS (Multiprotocol Label Switching) network is a standard protocol for connection SCADA systems to the Transmission communication network. The MPLS is based on MPLS switchers connected to transmission equipment like BG or SDH and from other side to the SCADA systems like Homeland security systems presented in HTB by DVR and video cameras or SCADA systems presented in HTB by different HMI (WIZCON, CIMPLICITY) and RTUs (MOSCAD, ACE, MODICON). MPLS switchers and SCADA components have IP address and provide good possibility to validate the CockpitCI project goals.

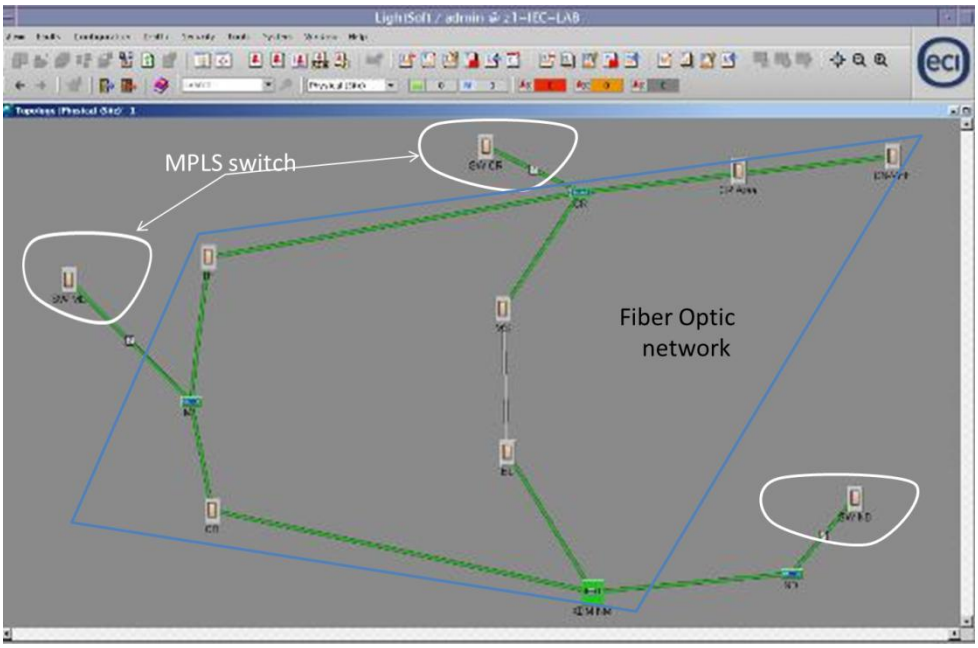


Figure 12: CCI Simulation Model Configuration

3.4.3 Defence strategy model

Defence strategy of CI model is based on detection of a deviation from baseline of behaviour and initiation response action. The ICS (Industrial Control System) defence model principles are presented in Fig. 13.

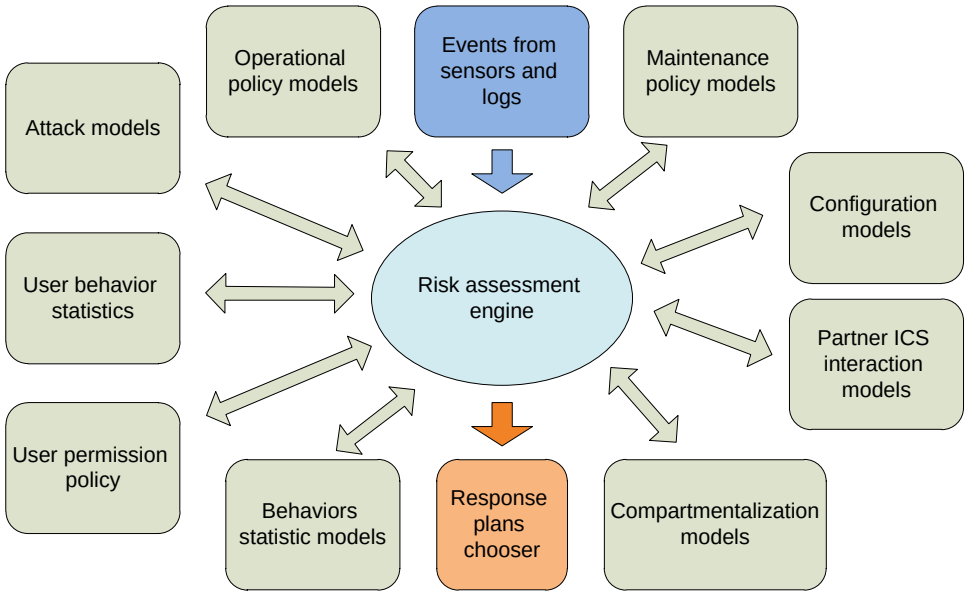


Figure 13: ICS defence model principles

The ICS (Industrial Control System) defence model includes the policies as follows:

- Operation policy models.

Operation policy models are based on:

a. Inventory and detail description of the manageable components (field devices, SCADA management system, network devices etc.)

b. Inventory and detail description of the management systems,

c. Set of the operational scenarios,

d. White list of operational commands per operation scenarios,

e. Black list of operational commands per operation scenarios,

f. Network protocols inventory per operation scenario.

- Maintenance policy models

Maintenance policy models are based on the capabilities as follows:

a. Set of maintenance scenarios,

b. Current maintenance scenarios,

c. Set of the components under maintenance procedure,

d. Maintenance procedure controller,

e. Infrastructure architecture for remote maintenance access.

- Behavior statistic models.

Behaviour statistic models include the capabilities as follows:

a. Network traffic statistic,

b. User login statistic,

c. Configuration change statistic,

d. Statistic of transition from different operation modes,

e. Maintenance statistics,

f. Attack statistics,

g. Virus statistics,

h. Process statistics per server/work station,

i. Installation/upgrade software statistics.

- Configuration models.

Configuration models include the capabilities as follows:

a. Systems inventory

b. Security patches inventory per applications, server, workstation,

c. Network devices inventory,

d. Electric devices inventory,

e. Topology,

f. Devices response signatures,

g. File system hierarchy per server/work station/PLC,

h. Processes inventory and signature per server/work station/PLC.

- User behavior statistic include the capabilities as follows:

a. Login logs per server/work station (time, IP, trace),

b. User action logs per server/work station.

- User permissions policy defines user permission per systems, applications, servers, workstations, network devices and etc. for every mode of operations and maintenance.

- Compartmentalization models define possibilities to isolate partly or fully compromised parts of ICS.

- Partner ICS interaction models include gateway architecture, policy of the protocols and content filtering.

- Attack models define possible attack goal, attack vectors, attack methods

Risk assessment engine will include the components as follows:

a. Compare events from sensors and logs against models,

b. Analyze possible risks,

c. Recommend response plan.

3.5 Verification Scenarios

3.5.1 Wizcon SCADA verification scenario

Wizcon SCADA verification scenario is presented in the following Table1. Wizcon SCADA verification scenario is realized as a set of high level commands that represents dispatcher's remote command and control operation of the ECI elements. The command execution (by THE SIMULATOR) is the subject to the state of the RTU that is responsible of the specific ECI element presented in Table1.

SCADA Commands	Interpretation of the simulator
"open CB"	set Circuit Breaker (CB) state to "open"; trace line sections downstream and set state (of each section) to "de energized"
"power line section"	set state of second switch (downstream) to "open" and enable power flow downstream
"power next line sections"	trace and energize line sections downstream (one step)
"set a cut"	set line section state to "fault"
"Isolate line section and restore power"	Set the state of the line section's switches to "open"; trace to border switch; energize line sections from border downstream

Table 1: Wizcon SCADA verification scenario example

Some examples of the verification scenarios

Scenario 1

Scenario 1 is a simulation of a fault management. The trigger is a cut in "Zuriel" HV line, which caused phase to ground current. Usually in this case "Zuriel" line protections would operate and trip Circuit Breaker(CB), but in this case the line protection didn't operate and as a result "out of limit" voltage developed in HV transformer neutral point to ground (coil).

Scenario1 shows a SCADA HMI fault management process executed by the dispatcher.

At the end of this example, the fault location will be found. The faulty line section will be isolated and service (power supply) will be restored to most of the customers. In each step the unsupplied energy will be calculated by the simulator. This set of commands is presented in the following Table 2.

Steps	SIMULATOR	SCADA
S1	*Initialize: Set a cut;*	
S2		*Alarm*
S3	Update Grid's state and calculate unsupplied energy	*Find the feeder that cause the fault*
S4	"	*Restore power to feeders*
S5	"	*Find the faulty line section*
S6		*ALARM*
S7	"	*Isolate line section and restore power from neighbour feeder*

Table 2: Set of Commands example

Detailed commands/data flow diagram and Actors (simulator and SCADA HMI) presented in Table.3.

Steps	Simulator	SCADA	Switch1	Switch2
S1	*Initialize: Set a cut in section 64* Table2. Set of Commands example *1BR-622R; This causes phase to ground current and voltage value on Coil to "OUT OF LIMIT"*		641BR	622R
S2		*Alarm*		
S3		*Find the feeder that cause the fault (end Alarm)*		
		Open CB	CB405	
	set CB state to "open"			
		ALARM		
		Open CB	CB406	
	set CB state to "open"			
		ALARM		

		Open CB;	CB407	
	set CB state to "open"; reset voltage value on coil to '1' (THE SIMULATOR could reset voltage value when the feeder is disconnected)			
		ALARM		
S4		*Restore power feeders*		
		Close CB	CB405	
	set CB state to "close"			
		end ALARM		
		Close CB	CB406	
	set CB state to "close"			
		end ALARM		
S5		*Find the faulty line section*		
		power line section1	CB407	435R
	Set line section state to "energize"			
		power next line sections	435R	641BR
	Set line section state to "energize"			
		power next line sections	641BR	622R
	Set line section state to "fault" and set CB state to "open"		641BR	48/635R
S6		*ALARM*		
S7		*Isolate line section ; Restore power from neighbour feeder (end ALARM)*	641BR	622R
	THE SIMULATOR could find the border switch which connects two feeders; Set the state of the second switch to "close". The effect on "Zuriel" is that its line sections become "energize" from border downstream	Isolate and restore power		

Table 3: Detailed commands description

3.6 Validation Scenarios

The validation scenarios evaluate that CockpitCI platform matching the User requirements stated in the Deliverable D5.1. Particular shape of the validation scenarios reflects lessons learnt during implementation of the CockpitCI. In every case, the final validation scenarios will be designed prior to the start of CockpitCI tool operation. The final version of the Validation scenarios will be presented in the deliverable D6.2 "Validation and Evaluation report".

Validation Scenarios describe the normal CI operation including the command and control process implementation, the CI operation under cyber-attack and the improvement of operators' the decision making process under cyber-attack using the CockpitCI tool.

Validation scenarios will be implemented during Task 6003.

The preliminary list includes the Validation scenarios as follows:

Electrical CI (ECI) Scenarios:

- Monitor loading in electrical grid
  The HTB includes sample measurements from the electrical grid. This data helps the supervisor in the control centre to monitor loading in the grid. The data repository will be in PI system. The user will be represented by PI system client that will provide HMI for queering the repository,
- Manage fault in the electrical grid.

The example of the Flowchart of the ECI validation scenario is presented in the Fig.14.

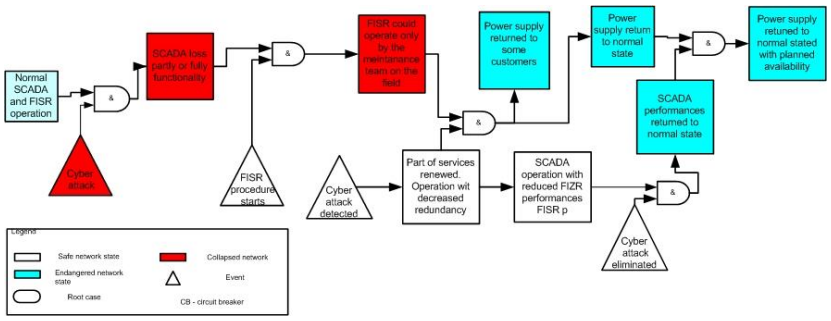


Figure 14: Example of the ECI validation scenario flowchart

Information and Communication Technologies CI (ICTCI) Scenario are including:

- Monitor communication to the RTU's and the status of RTU's,
- Monitoring of the communication elements status.

The HTB customisation for the ICTCI scenario includes PLCs (MOSCAD, ACE) that provide communication and control from maintenance centre to the RTU's. Communication equipment as well as the RTU's monitored by SCADA application based on WIZCON or Cimplicity HMI. The user in this scenario uses WIZCON and other SCADA HMI for execution queries to RTU's, and receives a report of their status.

Telecom CI (CCI) scenarios is presented in Fig.15.

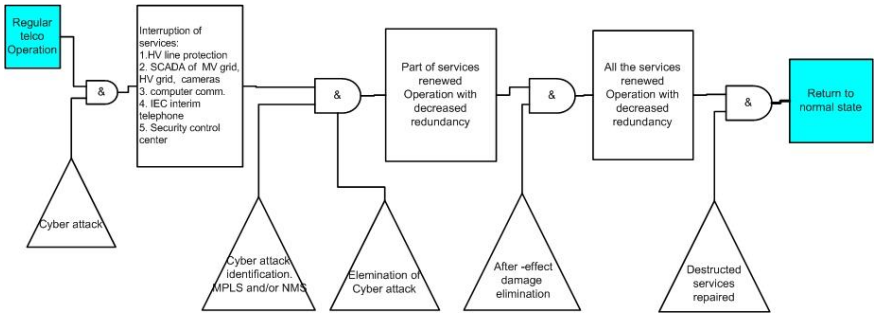


Figure 15: CCI validation scenario flowchart

Network management Infrastructure includes the following components:

- CCI manages communication. Its main service is to provide communication links between ICTCI elements. (e.g. computers PLC's and RTU's), VHF communication disturbances

  The HTB includes capabilities to simulate VHF communication disturbances like: VHF transmitting device that could block the VHF frequency used as a communication link. Thus, simulate VHF communication disturbances.

  While frequency is blocked, the user will use WIZCON HMI to execute open/close command to RTU. The command execution will fail and the user will get error indication in the WIZCON GUI.

- Failure in the communication backbone

  The HTB includes communication backbones' elements. These elements are managed by the LightSoft NMS (Network Management System).

  This Scenario simulates a fault in the BG element; the user in this scenario uses ECI WIZCON HMI to execute open command to a switch.

  The command execution will fail but the WIZCON user will not know the location of the fault. (I.e. if the fault location in ICTCI or in CCI)

The user will detect error indication of the BG element on the screen of the LightSoft NMS.

Smart House Scenarios includes as follows:

- AMI operations.
- Smart house (consumption and generation management).

Example of cyber-attack scenario and detection/mitigation scenario:

ECI possible cyber-attacks: Remote connection to MV SCADA HMI with admin permission.

Method of the attack:

a. Connect attack computer instead of a poor physical secure end-point device,
b. Scan network for accessible services,
c. Analyse ICS topology,
d. Identification of HMI servers,
e. Detect vulnerabilities of HMI servers,
f. Use vulnerabilities for access to HMI server,
g. Change service with admin privileges to the version with back-door function,
h. Delete trace of attack from logs.

Detection/mitigation method:

a. Install network IDS sensors for collection network traffic to and from HMI servers,
b. Compare network traffic with predefined policy (protocols, permitted commands etc.),
c. Install Host IDS on HMI servers,
d. Correlation rules Definition for detection of network traffic anomaly.

Examples of cyber-attacks goals:

- Attacker sends inaccurate/false information to CIs' operators, either to disguise unauthorized changes or to cause the operator to initiate inappropriate actions,
- Unauthorized changing or disabling alarm thresholds,
- Interfering with the operation of plant equipment, which can cause modification to safety settings,
- Blocking or delaying the flow of information through ICS networks, which could disrupt ICS operation,
- Making unauthorized changes to programmed instruction in local processors to take control of master-slave relationships between MTU's (Master Terminal Units) and FTU's,
- Modifying the ICS software or configuration settings,
- Infecting ICS software with malware,
- Blocking data or sending false information to CIs' operators. This action could distort a real status of CI and will cause of inappropriate decisions while management of CI,
- Overtaxing staff resources due to simultaneous failures of multiple systems

3.7 Validation Process Evaluation Results

After the CockpitCI tool will be successfully installed, verified and validated the next step will be the CockpitCI validation results evaluation and recommendations for the next steps. The evaluation will include the analysis of the problems that will invoke during CockpitCI validation, investigations by the project team, some important at achievements and project results as also as the benefits of the project.

During the CockpitCI project evaluation the conclusions of the different scenarios will be provided, and the results of the cyber-attacks scenarios will be analysed. The analysis will include the results of scenarios implementation for all the levels of ICS described in this document as also as all equipment used in the CockpitCI Validation system.

Considerable attention will be paid to analysis of the services stainability while cyber-attacks.

The evaluation results will be presented in the deliverable D6.3 "Validation and Evaluation report".

4 Conclusions

The document presents the CockpitCI Validation Plan developed before the validation process of the CockpitCI project l start. The final version of the Validation Plan includes the scenarios for CockpitCI verification and validation as also the schedule of the CockpitCI tool validation and CockpitCI Validation System description.

The final deliverable of the Validation Plan integrates the validation of the overall concept including functionalities and performances and includes the requirements to validation and test program for the CockpitCI tool. The Validation Plan is based on the Verification and Validation (V&V) process.

The Validation system environment includes the components as follows: CockpitCI tool, HTB, Verification and Validation Scenarios, Quality Centre (QC) tool and cyber-attacks simulation.

The HTB is a distributed environment that provides the possibility for parallel operation of the different users of the HTB. Customising to the CockpitCI project, the HTB provides to the project partners recourses for tool components development, test and integration; running different scenarios during CockpitCI tool validation; store validation results and return to the previous versions of scenarios. The Hybrid Test Bed provides to the CockpitCI developers with the following capabilities:

- Simulate operation scenarios (power grid and telecom) based on real SCADA and Network Management System (NMS), physical components of electrical and telecom infrastructure and simulated elements of electrical and telecom infrastructure,
- Collect and analyse real network traffic of heterogeneous networks (power grid, telecom network, SCADA),
- Test models and components for cyber-attack detection and identification,
- Test models and components for mitigation of cyber-attack influence on critical infrastructure,
- Identify and test vulnerable parts of CI with weak physical security and accessible to unauthorized people,
- Test effectiveness of countermeasure's plans,
- Test effectiveness of automatic reaction logics,
- Test CockpitCI system functionality,
- Define every partner as a user with a predefined access level.

Verification scenarios provide the cross reference of the tests and requirements as also the requirement management possibilities during the CockpitCI tool design, test and implementation. At the end of the verification process the CockpitCI tool will be tested to the entire stated requirements.

The CockpitCI tool validation scenarios implementation ensures that the tools' functions are implemented as needed in its intended environment, including its operational behaviour, and user interface. The hardware and the software will be validated at the system integration stage (Task T6002). This step is beyond the software and hardware verification processes. CockpitCI tool validation will determine that a system will execute all the things it should and will not do what it should not do. CockpitCI validation will be performed by an independent IEC team and will be performed in the validation system environment.

CockpitCI Validation Process managed by Quality Centre (QC) which is WEB based. Every partner has WEB access to view the validation process results and status. This document includes also the traceability of CockpitCI tools requirements and CockpitCI tool Test Plan implemented on QC tool used for requirements and validation process management during the CockpitCI project process.

Appendix 1 HTB Test Plan

1.1Test Name: HW & OS

Test ID: 133

Subject: Console_1

Status: Design

Designer: mkrimer

Creation Date: 21/04/2013

Type: MANUAL

Execution Status: Passed

Steps:

Step Name: Step 1

Description: Checking the following steps on machine **pc1-it-fp7**:
1.Check hardware connections of console: power is connected, monitor, keyboard and mouse connected properly

Expected Result: No problems occurred.

Step Name: Step 2

Description: Turn on the console
Machine testing - Run machine and see user name and password windows.

Expected Result: No error msg.

Step Name: Step 3

Description: check that the OS is Windows 7 coming up correctly (without any error msg.).

Expected Result: the hardware configuration report is matching to the requirements.

Step Name: Step 4

Description: Choose one (for instance 172.27.42.254) of the defined remote connections (connections defined previously) Make sure that the connections are established and you are capable to activate any application (i.e. Internet Explorer).

Expected Result: Application activated properly.

1.2Test Name: Hardware

Test ID: 136

Subject: FLD server

StatusL: Design

Designer: mkrimer

Creation Date: 24/04/2013

Type: MANUAL

Execution Status: No Run

Steps:

Step Name: Step 1

Description: Disconnect Servers (-2 Floor). There are 2 connections for every server.
Disconnect all the servers from the two connections and check if any of them reply.

1.3 Test Name: Ping Test

Test ID 137

Subject: FLD server

Status: Design

Designer: ybramly

Creation Date : 25/04/2013

Type: MANUAL

Execution Status: Passed

Steps:

Step Name: Step 1

Description: Make a Ping command to the relevant address (IP) and verify if the system react correctly.

Expected Result: ping OK

1.4 Test Name: Get Connection

Test ID:140

Subject: FLD server

Status: Design

Designer: mkrimer

Creation Date: 25/04/2013

Type: MANUAL

Execution Status: No Run

Steps:

Step Name: Step 1

Description: In order to get list of VM installed in the server the following steps will be implemented:
1. Start -> (Command Line) type: mstsc
2. Remote Desktop Connection -> type IP Address of TS for Server Admin
3. Fill User Name and Password
4. Answer Yes
5. Get in to "VMware vSphere Client"
6. Fill IP address of FLD server, User Name and Password and click "Login"
7. Choose "Virtual Machines" tab.
8. Add new column "IP Add" to the VM table by right click on the "view column" selection.

Expected Result: Getting in TS for Server Admin, Getting in "VMware vSphere Client", Receiving list of VM.

Step Name: Step 2

Description: In order to get list of Applications installed in the VM the following steps will be implemented:
1. Choose IP address of the machine (from the list of VM generated in step 1).
2. Remote Desktop Connection -> type IP Address of appropriate VM
3. Fill User Name and Password
4. Answer Yes
5. Go Start -> All Programs
6. Go Start -> Control Panel -> Programs and Features
(To Linux OP- connection through Putty Application. incase win OS use Remote console)
.**Expected Result:** Get the User/Pass screen.
Getting List of Applications installed in the VM (regarding to sections 5 and 6)

1.5 Test Name: Vicon Application Installation

Test ID: 143

Subject: Console_1

Status: Design

Designer: mkrimer

Creation Date: 02/06/2013

Type: MANUAL

Execution Status: No Run

Steps:

Step Name: Step 1

Description: 1. Login to the console No.1
2. Double click on the icon of "ViconNet" application
3. When Windows login displayed, push the "login" button

Expected Result: On the screen ViconNet the camera's pictures will be displayed according to the camera's number.

1.6 Test Name: WIZCON Operation

Test ID: 146

Subject: WIZCON

Status: Design

Designer: mkrimer

Creation Date: 09/06/2013

Type: MANUAL

Execution Status: No Run

Steps:

Step Name: Step 1

Description: 1. Access to VM pcfp721 (IP_172.27.42.254) through the Remote Desktop Connection.
2. Double click on the icon of "CockpitCI" on the desktop.

Expected Result: the diagram of the electrical network is show up.

Appendix 2 Requirement and requirement traceability

1. **UR_1 (Req ID 12)**

Requirement Parent: User Requirements

Requirement Type: Functional

Description: The CockpitCI tool shall improve the situational awareness and support the decision making capability of the SCADA operator in presence of cyber-attacks.

Validation Scenario Description: In order to test the CockpitCI tool to fulfill the requirement, the next three steps should be performed:

- **On the first stage all the CIs are operated according to the real Working procedures without cyber- attack, while CockpitCI tool are disabled. During this stage we have to check that all CI's are working properly**
- **On the second stage all the CIs are operated according to the real Working procedures during cyber- attack activated by the tester himself, while CockpitCI tool are disable. During this stage, SCADA operator should not receive a message/warning from the CockpitCI tool about occurrence of cyber-attack.**
- **On the third stage all the CIs are operated according to the real Working procedures during cyber- attack activated by the tester himself, while CockpitCI tool are enabled. During this stage, SCADA operator should receive a message/warning from the CockpitCI tool about occurrence of cyber-attack.**

Trace to:

Req: Name	Trace Comment
FR_15	
FR_16	
FR_19	
FR_22	

2. **UR_2 (Req ID 13)**

Requirement Parent: User Requirements

Requirement Type: Functional

Description: The CockpitCI tool *shall* improve the situational awareness and support the decision making of the cyber-security staff in presence of cyber-attacks.

Validation Scenario Description: In order to test the CockpitCI tool to fulfill the requirement, the next three steps should be performed:

• On the first stage all the CIs are operated according to the real Working procedures without cyber- attack, while CockpitCI tool are disabled. During this stage we have to check that no security event occurred.

• On the second stage all the CIs are operated according to the real Working procedures during cyber- attack activated by the tester himself, while CockpitCI tool are disable. During this stage, cyber-security staff should not receive a message/warning from the CockpitCI tool about occurrence of cyber-attack.

• On the third stage all the CIs are operated according to the real Working procedures during cyber- attack activated by the tester himself, while CockpitCI tool are enabled. During this stage, cyber-security staff should receive a message/warning from the CockpitCI tool about occurrence of cyber-attack.

Trace to:

Req: Name	Trace Comment
FR_13	
FR_14	
FR_17	
FR_20	

3. UR_3 (Req ID 14)

Requirement Parent: User Requirements

Requirement Type: Functional

Description: The CockpitCI tool *shall* improve business continuity and resilience of services delivered to Critical Infrastructure customers in presence of cyber-attacks.

Validation Scenario Description: Validation scenario based on simulation of outage of electricity supply to customers via medium voltage (distribution) network and resuming the supply using the FISR (Fault Isolation and System Restoration) procedures. In order to check the influence of CockpitCI tool on business continuity and resilience of services, we need to evaluate the following calculated parameters:

- **CAIDI- Customer Average Interruption Duration (in minutes)**
- **Unsupplied Electricity per Customer (in KVA).**

The FISR procedure should be performed on each of one of the following stages:

• On the first stage all the CIs are operated according to the real Working procedures without cyber- attack, while CockpitCI tool are disabled

• On the second stage all the CIs are operated according to the real Working procedures during cyber- attack activated by the tester himself, while CockpitCI tool are disable.

• On the third stage all the CIs are operated according to the real Working procedures during cyber- attack activated by the tester himself, while CockpitCI tool are enabled.

The tests results will be based on comparison of the calculated parameters between the three stages above.

4. **UR_4a (Req ID 15)**

Requirement Parent: User Requirements

Requirement Type: Functional

Description: The CockpitCI tool shall detect in near real-time cyber-attacks (including 0-days attacks) against the SCADA system.

Validation Scenario Description: In order to test the CockpitCI tool to fulfill the requirement, the next three steps should be performed:

• First stage all the CIs are operated according to the real Working procedures without cyber- attack, while CockpitCI tool are enabled. During this stage we have to check that no security event occurred.

• Second stage cyber- attack activated by the tester, while CockpitCI tool are enable. Time stamp of cyber-attack activation should be stored.

• Third stage, time will be measured until a message/warning from the CockpitCI tool about occurrence of cyber-attack will be received; this period of time is the detection time.

Remarks:

- **Assuming the cyber-attack generator will be repeatable regarding the composition of cyber-attack.**
- **In advance we assume that composition of cyber-attack includes 0-days attacks.**

Trace to:

Req: Name	Trace Comment
FR_1	
FR_2	
FR_5	
FR_6	
FR_7	

Req: Name	Trace Comment
FR_8	
FR_11	

5. UR_4b (Req ID 16)

Requirement Parent: User Requirements

Requirement Type: Functional

Description: The Cockpit CI tool *shall* isolate and react to cyber-attacks against the SCADA system.

Validation Scenario Description: In order to test the CockpitCI tool to fulfill the requirement, the next three stages should be performed:

- **First stage all the CIs are operated according to the real Working procedures, cyber- attack activated by the tester while CockpitCI tool are enabled. During this stage we have to check that security event occurred. Warning message should be received, including information about occurrence of cyber-attack and a segment of the network affected by the cyber-attack.**
- **Second stage the CockpitCI tool should display a list of the various options to act, that are relevant for operator choice. One of the relevant options should be isolation procedure activation.**
- **Third stage the operator should select the isolation procedure activation option. The CockpitCI tool should perform the procedure and report on success or fault result.**
- **Fourth stage is to verify that the network's affected area is surely isolated, by sending ping requests to units (RTU's for example) located in the affected area. If negative answer is accepted means that the area is isolated indeed. This step will perform only in case of success isolation procedure execution appears on third stage.**

Remark: the automatic execution of isolating procedure should be configurable option.

Trace to:

Req: Name	Trace Comment
FR_23	
FR_24	
FR_25	

6. UR_5 (Req ID 17)

Requirement Parent: User Requirements

Requirement Type: Functional

Description: The detection, isolation and reaction strategies of the tool *should* minimize the perturbations on QoS to customers in terms of business continuity and + of services to CI customers.

Validation Scenario Description: Validation scenario based on simulation of outage of electricity supply to customers via medium voltage (distribution) network and resuming the supply using the FISR (Fault Isolation and System Restoration) procedures. In order to check the influence of CockpitCI tool on business continuity and resilience of services, we need to evaluate the following calculated parameters:

- **CAIDI- Customer Average Interruption Duration (in minutes)**
- **Unsupplied Electricity per Customer (in KVA).**

The FISR procedure should be performed on each of one of the following stages:

- **On the first stage all the CIs are operated according to the real Working procedures without cyber- attack, while CockpitCI tool are disabled**
- **On the second stage all the CIs are operated according to the real Working procedures during cyber- attack activated by the tester himself, while CockpitCI tool are disable.**
- **On the third stage all the CIs are operated according to the real Working procedures during cyber- attack activated by the tester himself, while CockpitCI tool are enabled. The electricity network operator should act according detection, isolation and reaction strategy of CockpitCI tool.**

The test results will be based on comparison of the calculated parameters between the three stages above.

Trace to:

Req: Name	Trace Comment
FR_26	
NFR_4	

7. UR_6 (Req ID 18)

Requirement Parent: User Requirements

Requirement Type: Functional

Description: The CockpitCI tool *shall* identify the compromised sections of SCADA, ICT and in turn of the domain CI.

Validation Scenario Description: The CockpitCI tool will analyze the anomalies of SCADA, ICT and CI models and will alert on CockpitCI tool display the risk level (high, medium and low) of possible compromised

domain. In order to test the CockpitCI tool to fulfill the requirement, the next three steps should be performed:

- **On the first stage implement cyber- attack to the specific domain of SCADA (RTU, communication, HMI).**
- **On the second stage CockpitCI tool alert the risk level of abnormal behavior of threat compromised SCADA domain.**
- **On the third stage CockpitCI tool shall evaluate results of cyber-attack and alerting of compromised domain.**

Trace to:

Req: Name	Trace Comment
FR_13	

8. UR_7 (Req ID 19)

Requirement Parent: User Requirements

Requirement Type: Functional

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

Validation Scenario Description: In order to test the CockpitCI tool to fulfill the requirement, the next three steps should be performed:

- **First stage all the CIs are operated according to the real Working procedures without cyber- attack, while CockpitCI tool are enabled. During this stage we have to check that no security event occurred.**
- **Second stage cyber- attack activated by the tester, while CockpitCI tool are enable. Time stamp of cyber-attack activation should be stored.**
- **Third stage, all notices and warnings, arrive to the security staff about the security state of the CI, the location and severity of the attack, action performed and the result of the correction action performed, should be stored for future analysis. Evaluation of the entire collected data, including reaction time of CockpitCI tool, will make possible to decide about assessment of real time characteristics.**

Trace to:

Req: Name	Trace Comment
FR_13	
FR_17	
FR_20	

9. UR_8 (Req ID 20)

Requirement Parent: User Requirements

Requirement Type: Functional

Description: Cancelled.

10. UR_9 (Req ID 21)

Requirement Parent: User Requirements

Requirement Type: Functional

Description: The CockpitCI tool should not alter or interfere with the normal operations of the SCADA system

Validation Scenario Description: Validation scenario based on simulation of outage of electricity supply to customers via medium voltage (distribution) network and resuming the supply using the FISR (Fault Isolation and System Restoration) procedures. In order to check the influence of CockpitCI tool on normal operations of the SCADA system, the FISR procedure should be performed on each of one of the following stages:

- **On the first stage all the CIs are operated according to the real Working procedures without cyber- attack, while CockpitCI tool are disabled.**
- **On the second stage all the CIs are operated according to the real Working procedures without cyber- attack, while CockpitCI tool are enabled.**

The tests results will be based on comparison of the collected (measured and stored) parameters between the two stages above.

Trace to:

Req: Name	Trace Comment
NFR_9	

11. UR_10 (Req ID 22)

Requirement Parent: User Requirements

Requirement Type: Functional

Description: The CockpitCI tool *shall* not overload the SCADA operator with an excessive rate of false alarms.

Validation Scenario Description: The validation scenarios based on analysis of SCADA alarm log. The main purpose of this analysis is to separate between the real alarms and the false alarms.

Alarm log will be collected during two following stages of the test (while CockpitCI tool will be switched on):

- **On the first stage all the CIs are operated according to the real Working procedures without cyber- attack.**

• On the second stage all the CIs are operated according to the real Working procedures with cyber- attack.

The rate of the false alarms will be calculated by dividing number of false alarms by time duration of test.

Remark: the distinction between the real alarms and the false alarms will be made by SCADA and Cyber specialists on expertise bases.

Trace to:

Req: Name	Trace Comment
FR_3	
FR_4	

12. UR_11 (Req ID 23)

Requirement Parent: User Requirements

Requirement Type: Functional

Description: The CockpitCI tool *shall* be a scalable solution.

Validation Scenario Description: This requirement will be analyzed in document D6.2 "Validation and Evaluation Report".

Trace to:

Req: Name	Trace Comment
NFR_11	

13. UR_12 (Req ID 24)

Requirement Parent: User Requirements

Requirement Type: Functional

Description: The CockpitCI tool should cost reasonably.

Validation Scenario Description: This requirement will be analyzed in document D6.2 "Validation and Evaluation Report".

Trace to:

Req: Name	Trace Comment
NFR_12	

14. UR_13 (Req ID 25)

Requirement Parent: User Requirements

Requirement Type: Functional

Description: The CockpitCI tool shall be effective both on new SCADA HW/SW as well as legacy SCADA HW/SW.

Validation Scenario Description: In order to test this requirement two different test environments will be implemented:

"New" test environment – based on new SCADA HW/SW.

"Legacy" test environment – based on legacy SCADA HW/SW.

The "New" and "Legacy" test environments will be determined before the test start.

On the first stage, operator should activate CockpitCI tool and start on the cyber-attack on the "New" test environment.

Operator should collect all messages/info regarding the CockpitCI tool activities.

On second stage operator should activate CockpitCI tool and start on the cyber-attack on the "Legacy" test environment.

Operator should collect all messages/info regarding the CockpitCI tool activities.

On base of comparison of this collected information the test team will decide about effectiveness of CockpitCI tool both on new SCADA HW/SW as well as legacy SCADA HW/SW.

Trace to:

Req: Name	Trace Comment
NFR_13	

15. UR_14 (Req ID 26)

Requirement Parent: User Requirements

Requirement Type: Functional

Description: The CockpitCI tool shall be compatible and possibly integrable with other cyber security defense software.

Validation Scenario Description: Validation scenario based on a simultaneous activation of CockpitCI tool and "other" cyber security defense software, and analysis of the common work results. "Other" cyber security defense software will be activated during all stages in the test.

The tests composed of the following three stages:

- **On the first stage operator should activate cyber- attack, while CockpitCI tool are disabled.**

• On the second stage operator should activate CockpitCI tool without cyber-attack.

• On the third stage operator should activate CockpitCI tool and cyber-attack.

The conclusion based on the analysis of the alarms log, messages and any other occurrences during all three stages.

Trace to:

Req: Name	Trace Comment
FR_10	

16. UR_15 (Req ID 27)

Requirement Parent: User Requirements

Requirement Type: Functional

Description: The CockpitCI tool should not use the SCADA communication infrastructure, but should provide its own communications means.

Validation Scenario Description: This requirement will be analyzed in document D6.2 "Validation and Evaluation Report".

Trace to:

Req: Name	Trace Comment
NFR_9	

17. UR_16 (Req ID 28)

Requirement Parent: User Requirements

Requirement Type: Functional

Description: The CockpitCI tool shall provide an "intuitive" user interface that will provide the SCADA and security operators only with necessary information for decision making in uncertain situations.

Validation Scenario Description: On the first stage, operator should activate CockpitCI tool and start on the cyber-attack.

On second stage operator should collect all messages/info regarding the CockpitCI tool UI.

On base of this collected information the test team will decide about the intuitive issues of UI.

Trace to:

Req: Name	Trace Comment
FR_19	

Req: Name	Trace Comment
FR_20	

18. UR_17 (Req ID 29)

Requirement Parent: User Requirements

Requirement Type: Functional

Description: The CockpitCI tool should also improve synergies between SCADA control and cyber security.

Validation Scenario Description: Validation scenario based on simulation of outage of electricity supply to customers via medium voltage (distribution) network and resuming the supply using the FISR (Fault Isolation and System Restoration) procedures. In order to check the influence of CockpitCI tool regarding synergies between SCADA control and cyber security, we need to evaluate the following calculated parameters:

- **CAIDI- Customer Average Interruption Duration (in minutes)**
- **Unsupplied Electricity per Customer (in KVA).**

The FISR procedure should be performed on each of one of the following stages, while cyber- attack activated and CockpitCI tool are enabled:

• On the first stage only SCADA operator is function according to the real Working procedures

• On the second stage only cyber security operator is function according to the real Working procedures.

• On the third stage both SCADA operator and cyber security operator are operated according to the real Working procedures.

The evaluation of tests results will be based on comparison of the calculated parameters between the three stages above.

Trace to:

Req: Name	Trace Comment
FR_21	

19. UR_18 (Req ID 30)

Requirement Parent: User Requirements

Requirement Type: Functional

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

Validation Scenario Description: On the first stage configure the system on active mode and start on the cyber-attack. Operator should write down a list of whole activities of CockpitCI tool during the cyber-attack.

On the second stage configure the system on passive mode and start on the cyber-attack. Operator should write down a list of whole activities of CockpitCI tool during the cyber-attack.

On the third stage of this test, the operator should compare the two lists accepted in the previous stages. Check that no active actions made during the passive mode stage.

Trace to:

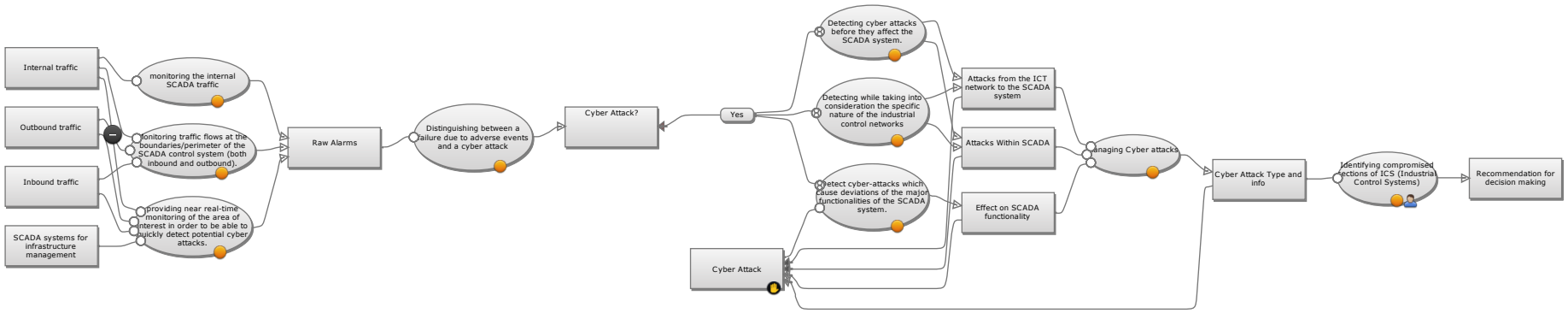
Req: Name	Trace Comment
FR_26	

Appendix 3 CockpitCI flowcharts derived from Visio process tool.

Cockpit

Detecting Real Time Cyber attacks

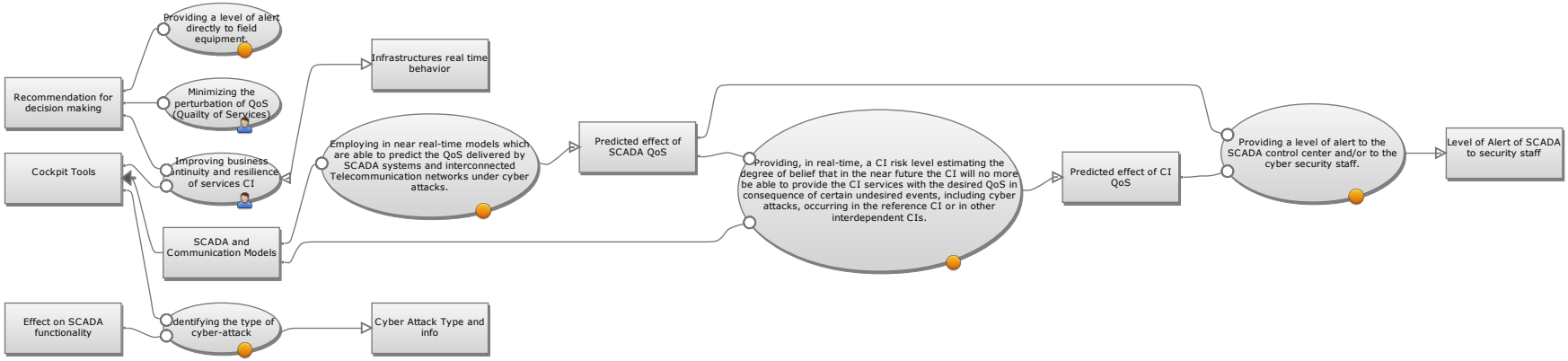
Last Save
8 minutes ago



Cockpit

Improving business continuity and situation awareness

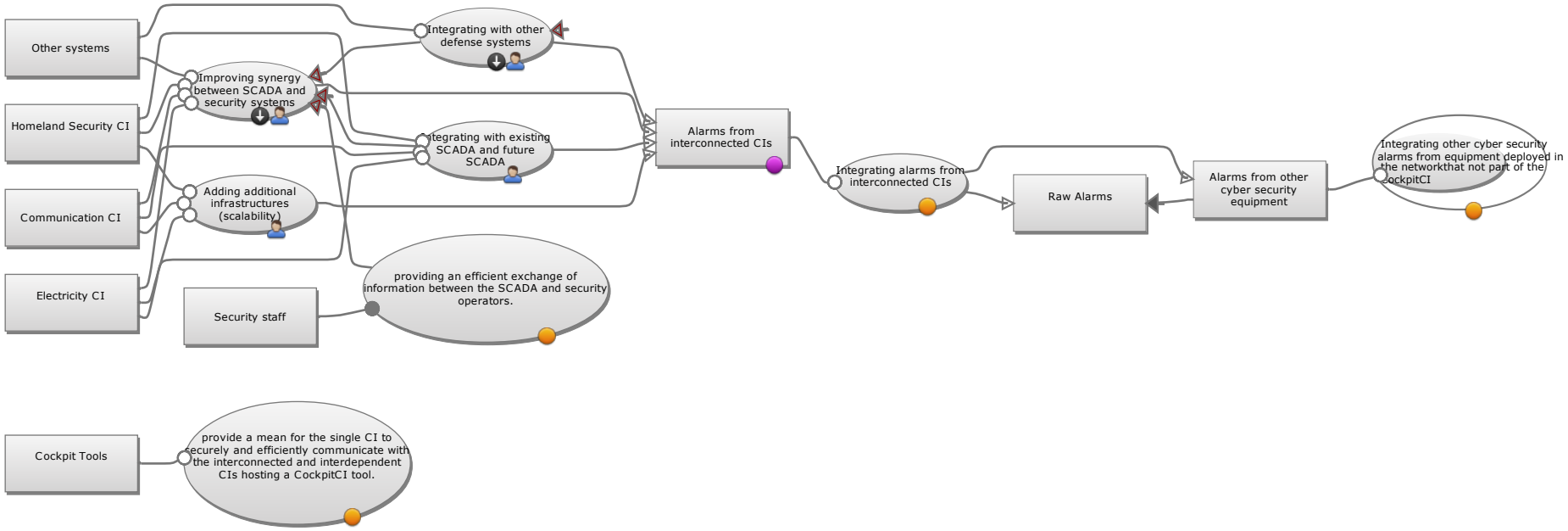
Last Save
14 minutes ago



Cockpit

Integrating with other systems

Last Save
15 minutes ago



Cockpit

Managing Risks at Real time for critical infrastructures(CockpitCI)

Last Save
2 minutes ago

Cockpit

Providing an intuitive user interface

Last Save
25 minutes ago