CockpitCI

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

1.1 Executive Summary

The CockpitCI project addresses the protection of Critical Infrastructures in the presence of cyber-attacks which may affect the SCADA systems. The CockpitCI vision identifies the need to complement business awareness with cyber-security awareness in order to reach a superior level of awareness (global awareness) and increase the business continuity of Critical Infrastructures (CI). Therefore the CockpitCI project encompasses a multi-layered cyber detection framework, capable of detecting security events or intrusion attempts on the entire critical infrastructure, together with a near real-time risk evaluation capability which determines the CI functionalities potentially impacted by cyber-attacks and faults, assesses the degradation induced on CI delivered services, provides decision support to the Operator and supports the activation of possible containment strategies. CockpitCI provides the means for a smarter and more effective graceful degradation of the CI thanks to a deeper understanding of how much of the infrastructure can be kept in operation safely in adverse situations and therefore maintain at least partial operation rather than total shutdown. CockpitCI is a security and business support solution, which can be provided with a variable degree of capabilities ranging from a purely passive monitoring decision support solution (suited also for legacy systems) to a more sophisticated solution capable of limited automatic reactions in predetermined situations. CockpitCI potential and perspective extend beyond cyber events and beyond the single infrastructure by taking into account interdependency effects among adjacent interdependent infrastructures.

The CockpitCI project has conceived and designed a solution which aims to provide increased situation awareness to operators, via modelling the effects of faults and cyber attacks and their propagation inside and outside of the Critical infrastructure, and makes it possible to keep the infrastructure running at partial operation even in adverse situations. The CockpitCI project has developed an integrated demonstrator which provides functionalities ranging from detection to decision support and reaction capability, and which comprises the following main parts:

- a multi-layered cyber detection framework, which includes a distributed heterogeneous sensing layer and two correlation levels which combine rule-based detection and machine learning algorithms;
- novel detection devices which are specific for the SCADA domain, i.e. field honeypots and shadow RTUs;
- a secure mediation gateway, which ensures transparent communication among CockpitCI components and secure communication with adjacent infrastructures;
- a risk predictor, which models and predicts the effects of cyber attacks and faults on the capability of the infrastructure to continue to deliver its services with a specified Quality of Service (QoS);
- smart RTUs, which have local situation awareness and can exhibit local behaviour such as entering a safe mode of operation;
- the HTB (Hybrid TestBed), which is a distributed and virtualised environment that provides the possibility for remote and parallel operation of the different users of the testbed.

1.2 Project context and objectives

The CockpitCI project addresses the protection of Critical Infrastructures in the presence of cyber-attacks which may affect the SCADA system. Industrial Control Systems (ICS), which include Supervisory Control and Data Acquisition (SCADA) systems, are normally used in industrial contexts such as utilities (electricity distribution and production, water supply and sewer processing, natural gas distribution), oil complexes or chemical processing. A SCADA system centralizes data acquisition and supervisory control; it comprises sensing devices which measure relevant parameters over the entire infrastructure, trained Operators who monitor and maintain the operation of the infrastructure according to Customers' needs, actuators which translate the Operator's decisions into specific control actions and a communication network which carries around sensor readings and control instructions across the infrastructure. Nowadays, ICS constitute a critical and strategic asset on which modern societies are fully dependent and yet ICS are being increasingly targeted by malicious attacks, therefore increasing the potential for catastrophic consequences. An attack could be performed in order to block the communication from central SCADA to local field equipments, in this way Operators would loose observability and controllability of the Critical Infrastructure; another attack could be performed inserting fake commands/measurements in the SCADA-field equipment communications (as happened with the STUXNET worm), in this way Operators could be induced to believe that they know the status of the infrastructure and that everything is normal, whilst the attacker is hampering with the infrastructure.

Critical Infrastructures are today severely exposed to and threatened by cyber-attacks. For decades the world of Industrial Control Systems (ICS) for CIs has evolved mostly on its own, lagging behind and ignoring the advances in information technology and cyber-security practices. ICS were a different world, with a very long obsolescence time, and this contributed to create the old SCADA platform paradigm in which security was not considered an issue and was implicitly guaranteed by obscurity and systems isolation. Under the pressure of cost reduction and market liberalization, this was no longer acceptable and Critical Infrastructures have in fact just emerged from a significant transition, i.e. evolving from proprietary and closed architectures to open, standards-based solutions, which are designed to ease interoperability with other similar platforms and different devices and platforms. 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 leads to very dangerous situations and this increased connectivity (with the Internet and other communication networks) exposes such systems to higher security risks. Therefore the need arises to increase business awareness with cyber-security awareness to reach a superior level of awareness (global awareness).

The CockpitCI project stems from the previous FP7 MICIE project, which has proved that increasing cooperation among infrastructures, sharing information about the operative levels of such infrastructures and sharing interdependency models increases their reliability and predictive capability of providing sensitive services. The MICIE approach is not enough to effectively counteract threats such as cyber-attacks; MICIE addresses the faults management to avoid risk cascading effects but not directly the causes of those faults and in the case of cyber-attacks this would imply always lagging behind the events. CockpitCI extends the MICIE philosophy by encompassing awareness for cyber-events.

CockpitCI aims to prove that the establishment of an efficient cyber oriented awareness, based on smart agents capable of detecting security events, anomalies or intrusion attempts into the ICS, will strengthen the business continuity strategy of the whole infrastructure. These agents provide in

fact an ICS security feed that can provide a broader insight into the security status of the whole infrastructure.

More specifically CockpitCI aims to improve the resilience and dependability of Critical Infrastructures (CIs) through the automatic detection of cyber threats and the analysis of such security events. CockpitCI aims to identify, in real time, the CI functionalities which are potentially impacted by cyber-attacks and assess the degradation of CI delivered services. CockpitCI aims to classify the associated risk level, broadcast an alert at different security levels, provide decision support to Operators and eventually activate a strategy of containment of the possible consequences of cyber-attacks. CockpitCI aims also to leverage the ability of field equipment to counteract cyber-attacks by deploying preservation and shielding strategies able to guarantee the required safety. By encompassing both the local, system-specific perspective and the global view at the CI level, CockpitCI provides the means for a smarter and more effective reaction capability, targeting a graceful degradation scenario, thanks to deeper understanding of how much of the system can be kept in operation safely in adverse situations and maintained at least in partial operation rather than total shutdown.

In the wider context where MICIE and CockpitCI strengths are combined, this overall capability is extended to the entire system-of-systems, i.e. to the ensemble of interdependent CIs, which can then operate more effectively and provide increased adaptation to adverse situations.

1.3 Main S & T results/foregrounds

The CockpitCI project has carried ahead an integrated solution concept which encompasses cyber detection and analysis, Quality of Service (QoS) modelling and simulation, risk prediction and reaction. A schematic diagram of the CockpitCI solution is shown in the figure below in terms of service components, information flows, databases and interfaces among components.

The bottom level retrieves and analyses information from the field - both from a cyber-security point of view (PIDS and SMP) and from a service point of view (Service Monitoring and Analysis Tools) to centralize it, in a dedicated format (with a specific granularity) in the SMGW database. The intermediate level is the SMGW and its database which centralize the relevant information from the field and (possibly) from neighbouring CIs. The top level is the expert services of CockpitCI (Risk Prediction Tool; Simulation etc…) which assess the risk for the CIs and provide relevant information to the Control room (and possibly to neighbouring CIs). An incident response team is included in the diagram to manage the communication between operational teams (SCADA operators and IT operators) to ensure a coherent response to events.

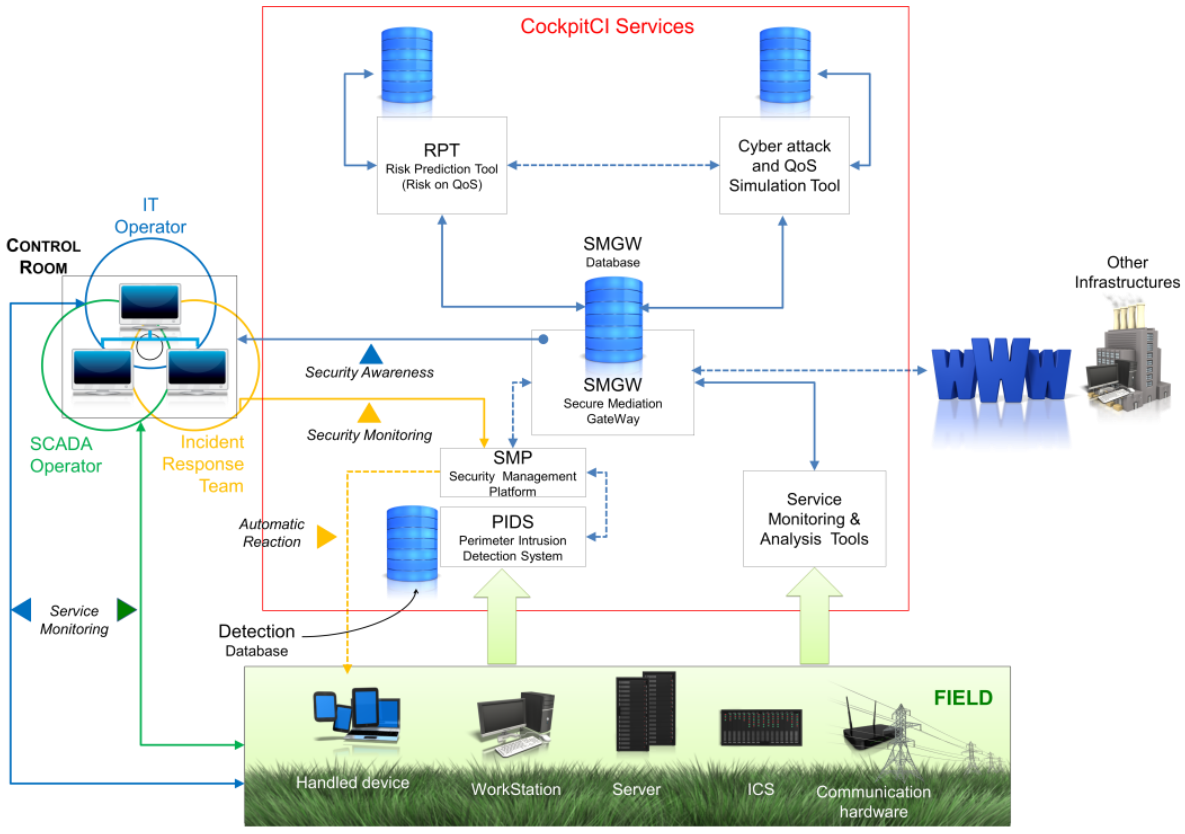
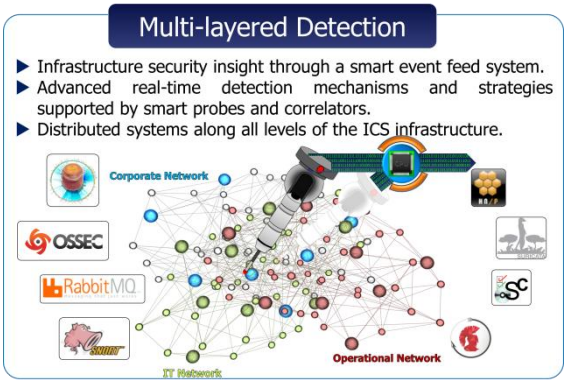


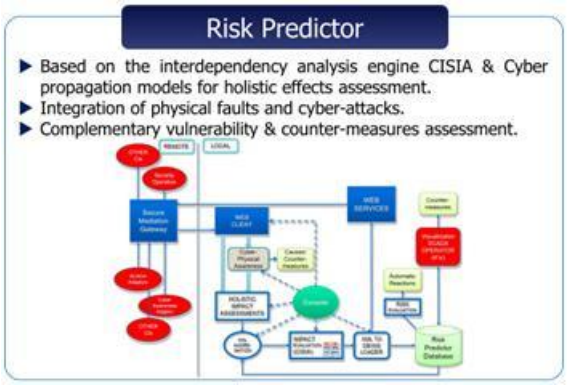
Figure 1: CockpitCI schematic diagram.

In the following a brief description of the main components and features of the CockpitCI project is provided.

The Cyber Analysis and Detection, a multi-layered detection framework, is one of the main blocks of the CockpitCI system. It performs many of the tasks traditionally associated with a Distributed Intrusion Detection System and is capable of detecting malicious network traffic which may disrupt the correct functioning of a SCADA system. The reference architecture encompasses both state-of-the-art and innovative SCADA specific concepts, techniques and devices. A new machine learning based approach for abnormal traffic event detection is also included in addition to rule-based topology and SCADA specific detection algorithms. Detection agents for intrusion detection and vulnerability assessment at local level, including both agents/adaptors/extensions for existing system components and specialized detection components to be added to the network, have been defined according to a modular and standard design especially in terms of reporting based on worldwide used IDMEF standard reporting format. Each of these detection agents will be able to (i) autonomously detect and, as much as possible, analyse security events and measure attack indicators and (ii) feed the upper layer with the data needed for advanced detection of distributed attacks or for in-depth analysis of suspicious security events.



The Integrated Risk Prediction Tool (IRP) is another main block of the CockpitCI system. It is a near real-time risk evaluation capability, fed also by the cyber-awareness layer, which helps SCADA operators to better evaluate and react to potential threats, in order to avoid cascading effects and keep in line with existing service level agreements and availability levels contractually established with customers. The Risk Predictor is based on CISIA, which is complemented with cyber propagation models in order to take into account the presence of cyber-attacks. CISIA is the main simulation engine based on a holistic / reductionist approach and capable of interdependency analysis.

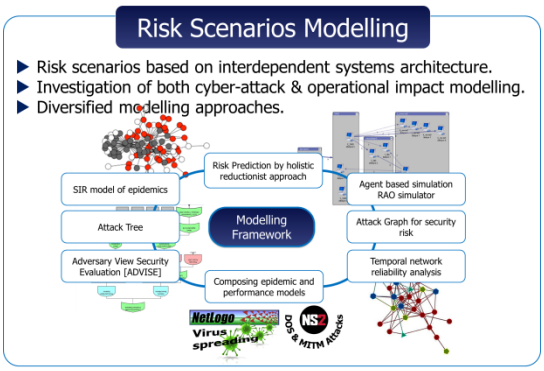


The Secure Mediation GateWay (SMGW), which is a secure exchange mechanism used to connect interdependent CIs and to manage the information dataflow among the system components, ensures scalability, security and heterogeneity.

A Reference Scenario has been specified to assess the awareness improvement for an Electrical provider in case of CockpitCI system implementation. The Reference Scenario is based on a Medium Voltage electrical grid, its SCADA system and a corporate network. The Reference Scenario includes topologies, main functionalities, main devices and main communications among devices, including communication protocols with special attention to TCP/IP based protocols; it also takes into account interdependencies and cyber security issues such as cyber threats, vulnerabilities, pre-existent cyber security policies, technical solutions and attack cases. This

scenario framework also includes cyber attack scenarios such as attacks on PLC/ICS devices, on telecommunication devices or on monitoring workstation which have been selected and instantiated during the test phase of the project.

A modelling framework, instantiated on the Reference Scenario, has been developed. The framework tends to represent, with different formalisms, models and tools, not only cyber attacks spreading or electric infrastructure functionalities but namely the cyber attack influence on the functionalities of the electric grid controlled by vulnerable SCADA system over a vulnerable corporate network. The modelling effort has so far confirmed the assumption that, at the state of the art, no single modelling technique has the credible modelling power and the analytical tractability to adequately deal with the QoS of the System of Systems under cyber-attacks. Cyber modelling in particular is a relatively young domain and high fidelity models seem to require fine grain models which are relatively difficult to build. Different numerical indicators of QoS of SCADA and in turn of the electrical grid to be evaluated along the different phases of a cyber attack have been identified.



Results and prototypes are also available regarding smart RTUs, where the term “smart” aims at autonomous adaptation to the surrounding environment; smart RTUs have the capability of recognizing malicious commands, and setting up strategies for automatic reaction, seeking cooperation among RTUs at local field level and with the Risk Predictor at global level.

And finally a significant achievement is the implementation, the fine tuning and the use of the Hybrid Test Bed Concept developed in the project framework. The HTB is a distributed and virtualised environment that provides the possibility for remote and parallel operation of the different users of the HTB.

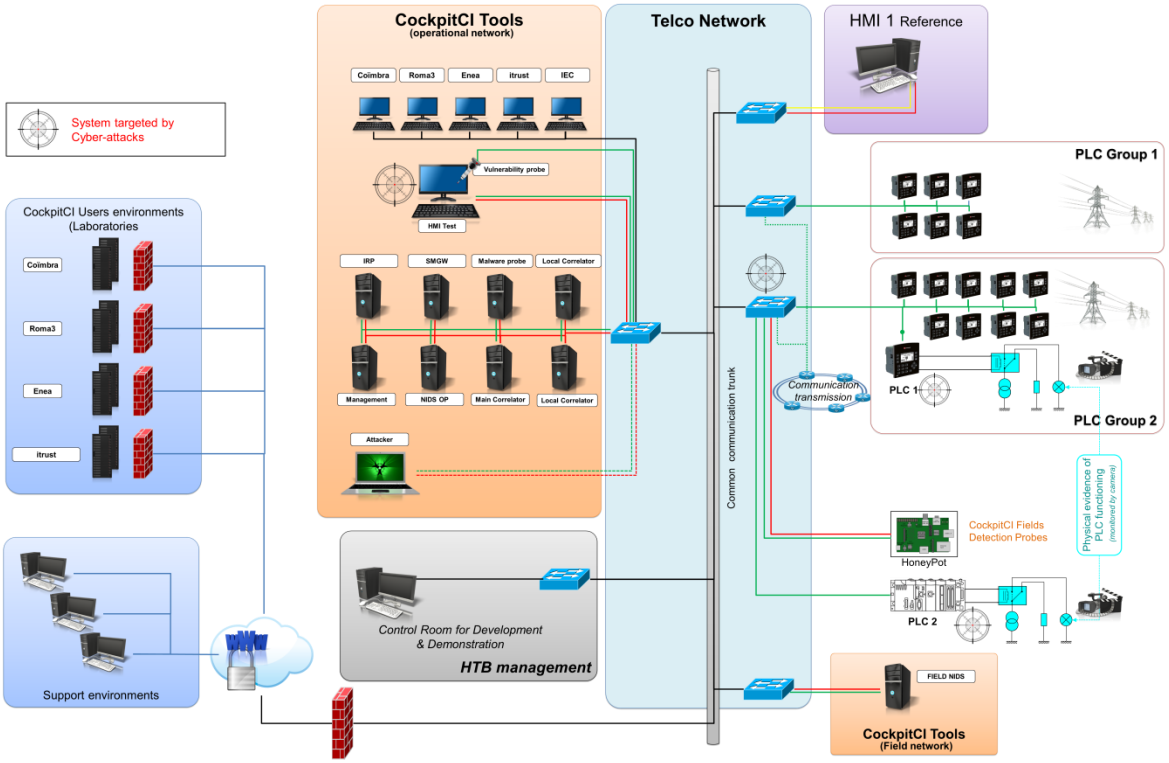


Figure 2: Deployment of CockpitCI system in Hybrid Test Bed

In CockpitCI project, the HTB provides, through virtualisation capabilities, a mirror image of a real critical infrastructure which can then be used to test the tools and methodology used in the project, to assess risk and simulate scenarios and to connect partners' labs together.

In the following, the main S&T results are described in more detail.

1.3.1 Integrated solution

The first contribution and innovation of the CockpitCI project is the design of the solution, oriented to promote a close integration of components from cyber detection to risk prediction and reaction. CockpitCI represents an additional layer of defence and awareness which can be overlayed on an existing architecture (including legacy system), without interfering with normal operations, to increase the awareness level of the single Critical Infrastructure or interdependent CIs. The capacity of integration of the solution is based on:

- An independent, modular and multi-layered detection service which captures and analyses the cyber information on the different networks of the infrastructure through dedicated probes and correlation engines.
- The secure mediation gateway SMGW which centralises and distributes all relevant information not only within the targeted CI but also from neighbouring CIs.
- The expert systems (prediction and modelling tools) which assess the QoS and the best solution of fault management process in case of operational incident according to the cyber risk evaluation.
- A dedicated HMI to give the right information to IT or SCADA operators.
- A graduated implementation of countermeasures managed by a dedicated team according to security and operational policy.

Last but not least the solution is designed according to a standardised approach (such as IDMEF, which defines an experimental standard for exchanging intrusion detection events) to be easily upgraded and integrated with already existing solutions.

1.3.2 Cyber Detection layer

The CockpitCI cyber-detection framework brings state-of-the-art SCADA-oriented cyber-security awareness into the ICS infrastructure, providing an event feed that offers a broad insight into the security status of the whole infrastructure. For such purpose, the cyber-detection architecture incorporates several advanced real-time detection mechanisms and detection strategies, distributed along the different levels of the ICS infrastructure, such as detection agents, specialised field adaptors, correlation mechanisms, unsupervised anomaly detection techniques and also aggressive usage of topology and system-specific detection mechanisms. It also aims to improve upon the state-of-the-art on ICS security by introducing new innovative security resources, which promise to be effective also against Stuxnet-like threats.

A near real-time risk evaluation capability, which is built on the cyber-awareness mechanisms, helps SCADA operators to better evaluate and react to potential threats, avoiding cascading effects, in line with existing service level agreements and availability levels contractually established with customers. This aims at reshaping the boundaries of the ICS and cyber-security contexts, in such a way that it becomes possible for both to work in tandem.

Ultimately, the CockpitCI Perimeter IDS (Intrusion Detection System) corresponds to the integration of the mechanisms for the CockpitCI Cyber Detection and Analysis Layer components (cf. Figure 3).

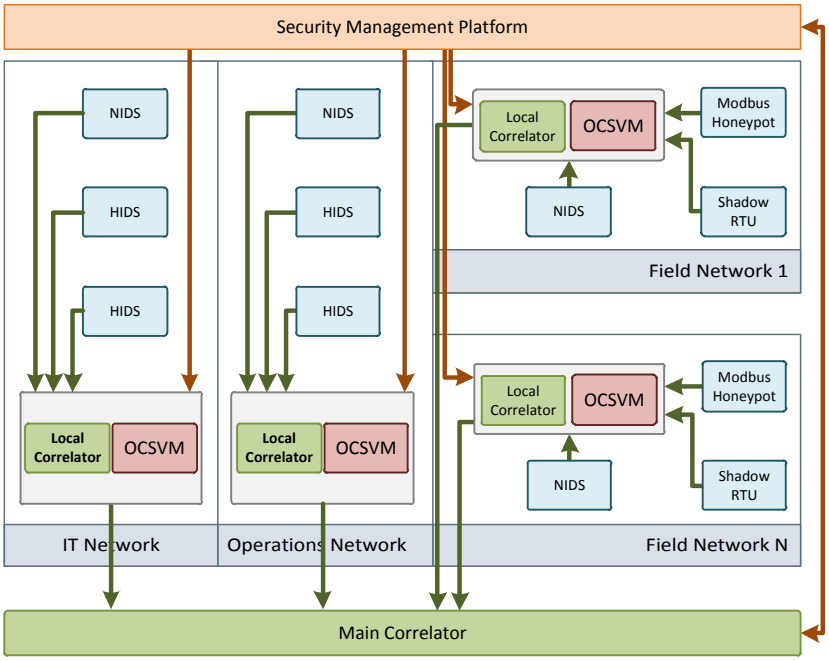


Figure 3: The CockpitCI Cyber Detection and Analysis Layer. (red flows=management, green=eventing)

The CockpitCI PIDS incorporates several advanced real-time detection and analysis mechanisms, integrated to constitute a cyber analysis and detection layer for the CI. It is structured along the three different zones of the CI, each one with its own internal security perimeter: the Field Network, SCADA Process/Operations Network, and the IT (Information Technology) Network. For each zone, the PIDS has the ability to deploy agents and security policies customized to the specific needs and characteristics of each network scope.

The implemented components comprise the components from the network scopes as well as the management network to connect the former components to the management server, which is part of the Security Management Platform. This includes the Detection agents and field adaptors (including agents, adaptors and extensions for existing system components, as well as specialized network probes and honeypots) and the Distributed Multi-zone, multi-level correlation and analysis structure that processes the information provided by the security sensors, processed by a distributed architecture of multi-level correlators, complemented by machine-learning capabilities, in the form of One-Class Support Vector Machine (OCSVM) anomaly detection modules.

The Security Management Platform (SMP) is responsible for managing all the components involved in the solution. It includes the mechanisms for managing the security and components of the infrastructure, being also responsible for the maintenance and management of monitoring probes such as IDS and the analysis components.

Implementation of the Detection and Analysis Layer

The analysis components of the PIDS provide a way to extract information from the data collected by the agent layer or directly from network traces. These components are arranged in a two-level architecture with local instances fine-tuned for each network scope.

Local and Global Correlators

Local correlators perform the first step of correlation, by filtering and reducing the number and noise of the alarms generated by the detection layer while, at the same time, providing a mechanism for security event generation that is able to filter, process, and relate events within a network segment. This provides the means to implement event reduction capabilities, aggregating alarms generated by two or more detection agents or multiple events from the same source.

Local correlators receive the events from local detection agents (for example HIDS) on their network scope and process them accordingly with a set of rules, and forward significant results to a global correlation engine. After local correlation, events are sent to the global correlators and from there to the SMN, by using the Intrusion Detection Message Exchange format. IDMEF defines an experimental standard for exchanging intrusion detection related events. As a standard, it provides a uniform and vendor-independent mechanism to provide communication between different agents such as NIDS or honeypots.

Local correlators receive events from the different agents such as NIDS, HIDS, and honeypots, among others. These agents are distinct, according to network zone, in which the local correlator is positioned. Despite the range of different agents, the local correlator uses the same interface for all of them, as messages are received through an Event Bus (based on a Message Queueing System). This interface allows subscribing to the events published by the agents. Local correlators also have an agent adaptor interface that allows for management, via the SMP.

Regarding the event interfaces for the main correlator there are several different types: one to receive events from the local correlators and another one to send events to the SMP, both using an Event Bus. As local correlators have already previously processed received events, the main correlator can focus on Multi-Step, Attack Focus Recognition correlation as well as Alert Prioritization. A management adaptor provides the interface for the SMP to configure the correlator (cf. Figure 4).

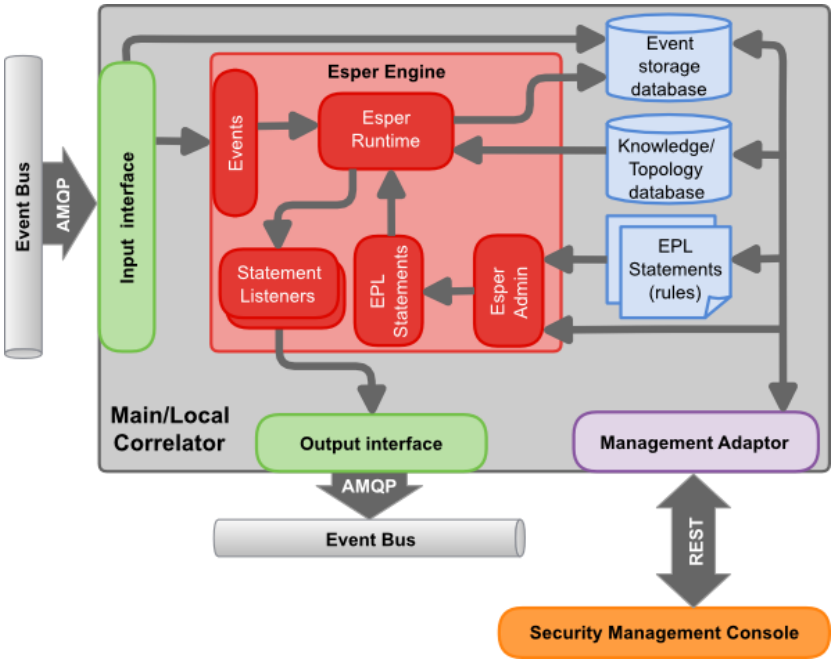


Figure 4: Overview of the Correlator Architecture.

One-Class Support Vector Machines (OCSVM)

OCSVMs (One-Class Support Vector Machines) are a natural extension of the support vector algorithm to the case of unlabelled data, especially for the detection of outliers. However, unlike SVM or any another classification algorithm, OCSVM does not need any labelled data for training or any information about the kind of anomaly it is expecting for the detection process. OCSVM principles have shown great potential in the area of anomaly detection Moreover, OCSVM is capable of handling multiple attributed data, which is well suited for SCADA systems.

The advantages of the OCVSM component are manifold: since OCSVM does not require any signatures of data to build the detection model, it is well suited for anomaly-based intrusion detection in the SCADA environment. Since the detection mechanism does not require any prior information of the expected attack types, OCSVM is capable of detecting both known and unknown (novel) attacks, besides being robust to noise in training sets. Also, algorithm behaviour can be

controlled and fine-tuned by the user to regulate the percentage of anomalies expected (thresholds, as defined via SMP, via the OCSVM management adaptor).

Detection Agents

The detection agents are the lowest level of the detection layer. Their purpose is to gather information from the system. As the format of information provided depends on the type of detection agents used (type of probe), adaptors allow the acquisition of data from the system in a recognised format. The detection agent operation workflow is depicted in Figure 5.

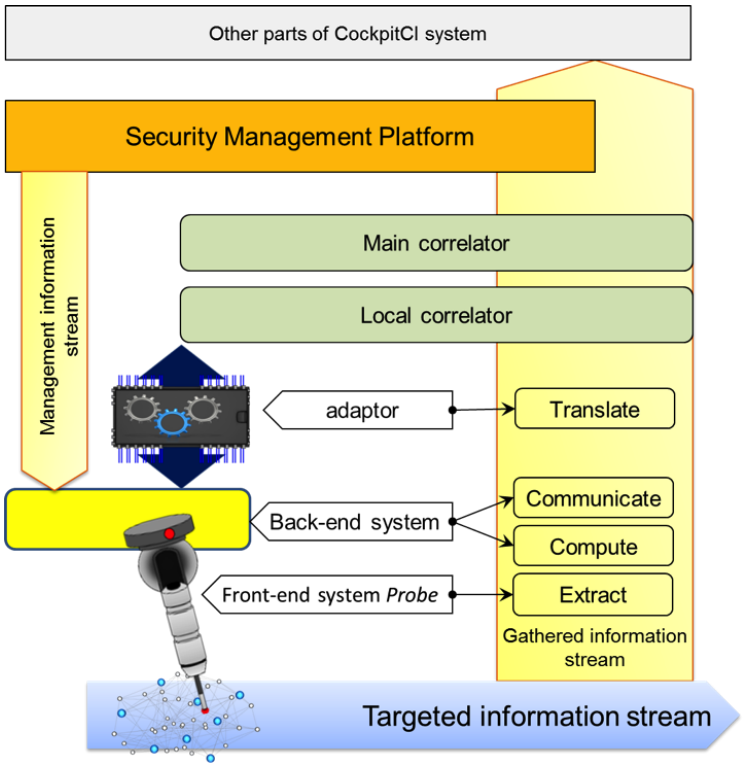


Figure 5: Operation Workflow for Detection Agents.

Detection agents and adaptors are essential to gather information, normalize it and feed it to the local correlators of the detection layer with input data regarding suspicious activity. The PIDS encompasses several kinds of probes and detection agents. The most relevant of these are next described:

- **Network IDS:** the perimeter for each network scope is monitored using NIDS components for each one: IT Network NIDS, Operations Network NIDS, and Field Network NIDS. These have interfaces to report the security events to the corresponding zone correlator.
- **Host IDS:** the Host IDS is deployed in the hosts/servers of the system. It is capable of reporting anomalous behaviour in the machine where it is deployed.
- **Honeypots**: acting as decoys and being capable of detecting attackers probing the network, honeypots provide another source of data for correlation. There are three types of honeypots: IT Network, Operations Network, and Field Network honeypots.
- **Shadow RTU**: the Shadow RTU is a low-cost device deployed in parallel with a PLC or Remote Terminal Unit (RTU), being capable of transparently intercepting its communications control channels and physical process I/O lines to continuously assess its security and operational status. The proposed device does not require significant change to the existing control network, being able to work in standalone or integrated within an ICS protection framework.
- **Exec Checker (linux hosts):** capable of detecting malicious network frames by sniffing the

traffic, the Exec Checker (in active or passive mode) captures the different parts of an executable in the network traffic to recreate the file and to send it to an analysis tool.

- **Output Traffic Controls (linux hosts):** capable of detecting Remote Access Trojans, this specific tool regularly scans system components to check if a remote access toolbox has been installed on components to facilitate external attacks.
- **Vulnerability Checker (windows hosts):** this tool provides a regular control of system vulnerability to check if the monitored systems are vulnerable or not according to an updated database. This tool can be customized for IT or SCADA host profiles.
- **Configuration Checker (linux/windows hosts):** this tool provides a regular control of system configurations to check for unauthorized modification.
- **Behaviour checker (linux/windows hosts):** capable of detecting attacks/threats by analyzing low-level hardware/software behaviour, this specific family of detection agents retrieves hardware/software information, such as temperature and CPU (Central Processing Unit) activity, in order to avoid accidental or malicious outage.

Security events generated by detection agents are encoded using the IDMEF format. All detection agents have a separate channel (another interface or secure channel) for management purposes, which enables the security staff to adjust the configurations with the scenario requirements via the SMP. The detection agents send their messages by means of an Event Bus described in the following section, which also details the management interfaces for the agent adaptors. These interfaces (eventing and management) were designed to ease integration of several types of detection capabilities (such as antivirus) by providing wrapper components for event generation and the management API.

1.3.2.1 Significant results

The most significant result relates to the implementation of a Distributed IDS architecture (the Cyber Detection and Analysis Layer), which is designed from the ground up for ICS and other Critical Infrastructures. By resorting to a mix of context-specific tools and techniques, together with generic security mechanisms it was possible to create an innovative solution encompassing advanced (in some cases, beyond the state-of-the-art) cyber-detection capabilities.

Moreover, the use of rule-based and anomaly detection capabilities make it capable of dealing with a wide range of threats, including rogue threats (which can only be detected by inference from behaviour and operational information). This accomplishment was only possible due to the contribution of a group of people with different expertise in areas such as cyber-security and machine learning.

To build the CockpitCI PIDS, several significant milestones were achieved:

1. Full development of the PIDS
2. Development of ICS-specific detection and analysis techniques and tools: the SCADA-specific Honeypot and the ShadowRTU
3. Development of a flexible testbed capable of providing an evolution path towards the integration stages, also providing a demonstration vehicle for innovative concepts.

PIDS

The CockpitCI Dynamic PIDS provides the core cyber-analysis and detection capabilities, being responsible for continuously assessing and protecting the electronic security perimeter of each CI. It was developed and integrated accordingly with the CockpitCI system architecture (see Figure 6). Integration testing, with both the Secure Mediation Gateway and the Integrated Risk Predictor has taken place, also taking a waterfall-style approach to API refinement and feature implementation, by feeding back test results to implementation teams.

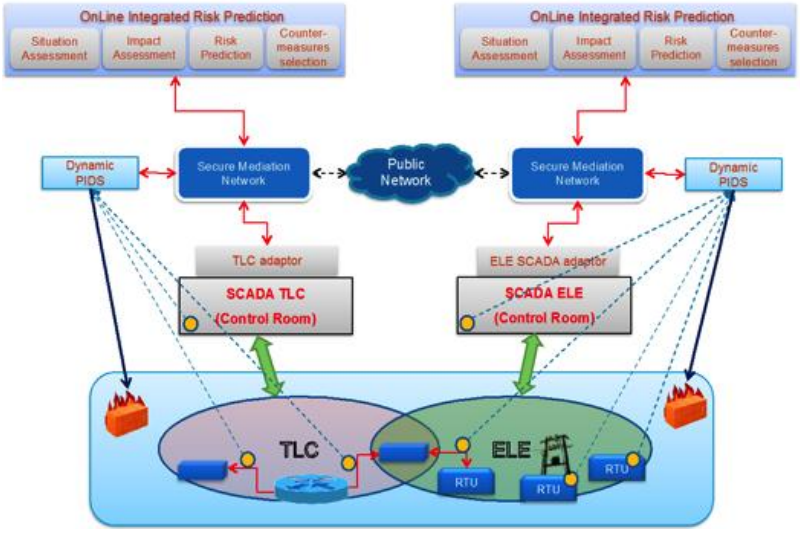


Figure 6: PIDS within the CockpitCI Architecture.

ICS-Specific Detection and Analysis Techniques and Tools

When it comes to their fundamental governing principles, ICS and ICT infrastructures have differences that are deeply rooted in their own specific characteristics, as noted by ISA-99; namely, an inverted set of priorities which is one of the main causes of SCADA security problems. For ICS, availability comes first, even if at the cost of integrity and confidentiality – the opposite of ICT.

The differences between the ICT and ICS contexts mean that there is no "one size fits all" solution when it comes to choose and deploy security mechanisms. Nevertheless, importing solutions from the ICT world is often a necessity, which might lead to undesirable side effects. The fundamental premises for ICT security tools and commonplace lifecycle management procedures, such as patching and updating a system, can become troublesome in an ICS when faced with situations such as the impossibility, the high cost of stopping production or even the explicit prohibition by the system's manufacturer, as it may happen with operating system updates or patches not previously certified by the equipment provider. Moreover, mature systems are often kept in operation far beyond their projected lifetime, constraining the implementation of some security measures, as existing equipment may lack the necessary requisites.

Altogether, this situation prompted work towards the development of domain-specific cyber-security mechanisms for ICS. This is one of the main objectives of the CockpitCI project, which focuses on improving the resilience and dependability of CIs, by detecting cyber-threats and sharing security information among CI operators. Amongst these (as several others may be pointed out, related to ICS protocol and infrastructure vulnerability discovery and mitigation) two particular achievements stand out: the SCADA Honeypot and the Shadow RTU.

The SCADA Honeypot

One of the innovations of the CockpitCI is the SCADA honeypot, designed to operate in the process control network of a SCADA/ICS system, coexisting with the existing array of PLCs, RTUs and sensors/actuators that populate the network, binding to the network's unused IP addresses. Its fundamental operating principle is based on the assumption that, by faithfully emulating the behaviour and service footprint of a commercial PLC, the network honeypot is able to faithfully persuade an attacker that it is a worthwhile target, acting as a decoy which actively reports any suspicious activity, by reporting events to the distributed IDS of the ICS, where they will be processed and correlated.

The SCADA honeypot is designed to behave and operate as a PLC, being designed to run on a SBC (Single Board Computer), thus being a cost-effective solution. Under normal conditions, the honeypot waits for a connection attempt from someone probing the network or accessing it with the intent of impersonating a master station. In practice, any attempt at contacting the honeypot device

may potentially generate a security event since, by definition, any activity in the honeypot is illegal and unauthorized (with the possible exception of management operations).

The proposed architecture (see Figure 7) is generic and compatible with the majority of SCADA protocols. However, Modbus was selected as the preferential protocol to be supported in the proof-of-concept prototype we developed, due to three factors: standardization, popularity and because it is based in an open specification, whose documentation is easily obtainable. For this reason, from now on we will specifically mention Modbus components, even though those components could be easily switched to add support for other SCADA protocols.

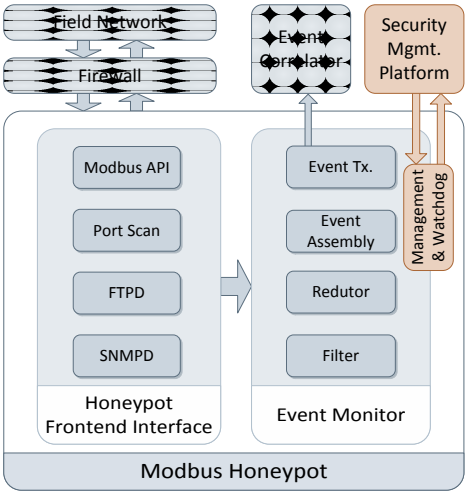


Figure 7: SCADA Honeypot Architecture.

The SCADA honeypot is based on a hybrid architecture, in the sense that it runs both simulated and complete implementations of services commonly available on PLC devices. To start with, there is a frontend module emulating the functional interface of a PLC. Its components are:

- A **Modbus API module** that specifically implements the Modbus TCP or IEC 104 protocols, widely used in ICS systems. The protocol operation is easy to understand: a master station sends commands (mostly read or write operations in the majority of situations) to a RTU/PLC who responds to them. The master station uses them to poll and change register values from the RTUs/PLC. Like a real PLC, the Modbus API module implements variables (registers) for storing values, enabling an attacker to interact with it, polling and changing the values, with the honeypot responding to the attacker's requests with the corresponding response.
- The **FTP and SNMP modules** respectively provide file transfer and management services commonly found in various Modbus PLCs. Each module has also a program monitoring the services' logs. The program is aware of any entry in the logs and is capable of reporting it to the Event Monitor for further analysis.
- For a better coverage of interactions, a **Port Scan module** is included in the architecture. This module isn't directly related to the SCADA technology context, being capable of capture generic network interactions, detecting the presence of an attacker. It listens to the remaining ports not covered by the other modules (Modbus API, FTP and SNMP),

The event monitor module is responsible to generate, filter, reduce/aggregate, normalize and transmit security events. Its components are:

- The **Filter and Event reduction** and aggregation modules preprocess security events, optimizing system resources (e.g., processing and network) and contributing to increase the scalability of the solution up to larger ICS network scenarios.
- The **Filter Module** is used to filter relevant events according to previously defined

configurations, which are stored in a file that is read when the module starts or by a watchdog module request. The filter module can, for example, discard events of no interest. Relevant events are next sent to the event reduction and aggregation module, which processes events in order to aggregate them by similar characteristics (for instance, grouping related events).

- The **Event Assembly** module is responsible for creating the security event messages, using a standardized format. The event message structure is based on IDMEF messages, which are sent using a secure channel between a sensor and a processing node, in this case the honeypot and the event correlator (which is responsible for event processing and correlation), respectively.

The honeypot contains a module for remote management. This module allows the security staff to modify the honeypot configurations (for example, Filter and Event reduction and aggregation modules configuration) from an authorized device. This is the only authorized connection to the honeypot. A watchdog sub-module also allows some actions to be remotely performed (such as restarting a module). The connection to the watchdog module is protected by a secure channel and authenticated in both ends, using the Transport Layer Security (TLS) protocol.

Shadow RTU

Also, during the development of the CockpitCI cyber-security detection framework, the CockpitCI team was faced with the problem of effectively protecting PLCs and RTUs. While playing an important role in the ICS context, such devices often lack adequate security mechanisms, having been successfully targeted in the past by a wide array of attacks, such as flooding, buffer overflow exploits or man-in-the-middle, just to mention a few. To address this problem, several authors have proposed the use of techniques such as bump-in-the wire VPNs, tight access control list mechanisms or introducing mutual authentication – countermeasures whose deployment is not feasible in all scenarios, for reasons such as latency overhead, reliability or the need for introducing profound changes on well-established protocols and architectures.

This situation has led to the research of an alternative for PLC/RTU security, capable of providing continuous device monitoring with minimal disruption: the Shadow RTU. The Shadow RTU is a device that is attached in parallel to RTU/PLCs, intercepting the command flow and physical process interfaces to assess their correct operation. It is transparent to the production system, requiring minimum changes to the existing architecture and, since it is out of the critical control path it cannot interfere with the operation of the system, also minimizing any other potential impact on the monitored device from an eventual malfunction.

The SCADA protocols that provide data and control synchronization between devices and supervisory/master stations range from simple, polling-based, operation (Modbus, IEC-104) to more sophisticated models, based on eventing (as it is the case for DNP3). The Shadow RTU is able to capture and decode the protocol information flow, correlating this information with the status of the physical I/O modules that interface with sensors and actuators on the field. This enables the possibility of implementing a redundant security-checking mechanism that follows a “black box” approach regarding the analysis of the monitored device.

The Shadow RTU prototype which has been build has several security capabilities, namely: intercepted command stream processing (enabling the creation of closed loop between command/control and the field), continuous network flow monitoring, message integrity/trust checks and abnormal behaviour detection. Apart from these benefits, the SSU can also provide information on the operational and health status of the device. Once the information is collected, the Shadow RTU may feed it to an SIEM or it may perform first-stage correlation itself and generate security events to the Security Control Room or SIEM, reporting anomalies that are taking place at the moment. A heartbeat mechanism ensures that the Security Management Platform of the SCADA operator is able to check the status and reachability of the Shadow RTU. The heartbeat, management, message checking and eventing mechanisms are provided on a

separate network for out-of-band operations, connected to a network interface of the Shadow RTU that is physically separated from the one used for security monitoring purposes.

1.3.3 Secure Mediation GateWay

The main S&T (scientific and technical) results of the Secure Mediation Gateway are the design and development of a modular, heterogeneous and secure exchange mechanism, able to establish and manage a federated security network across distributed and decoupled data sources. Modularity refers to the architectural design so that security mechanisms can evolve together with the evolution of the threat, heterogeneity refers to the fact that suitable heterogeneous technologies have been selected to support the specific requirements of each interface and security of course refers to the security mechanisms that are envisaged. The Secure Mediation Gateway manages the communication with components internal to the CockpitCI system as well as the communication with federated entities over the Internet. The key features are the following:

- the SMGW operates as a centralized security policy element, capable to control the security policies across different domains and designed so that only the managers of CIs have the full control of security policies and constraints;
- in order to assure the decoupling among service consumers and providers, the SMGW adopts the Web services approach and it is designed to enable a seamless and selective dispatching of messages among the entities connected through the SMGW using different interfaces according to the capabilities and requirements of each end-point;
- the SMGW implements the Web Services architecture using both SOAP and, at the same time, REST services. The main SOAP advantage relies in the definition of a very strongly typed messaging framework; every operation provides a service explicitly defined along with the XML structure of the request and the response end-point for that operation. The main advantage of REST is the ease of implementation, agility of the design, and the lightweight approach in resource consuming;
- the communication with federated entities over the Internet (interSMGW) is based on the message broker approach in order to manage the subscription/publishing of information to/from multiple SMGW instances in both synchronous and asynchronous mode;
- the federation of SMGW allows a dynamic management of security where the security manager of each federated domain can exchange policies with others modifying rules and privileges. Each change of the security configuration implies a reconfiguration in the capability of publishing and consuming services among the nodes of federation.
- in order to deploy an additional security element the use of a DeMilitarized Zone (DMZ) has been included in order to control all the ingoing and outgoing connections across the SMGW and external entities federated over Internet;
- the communication internal to the SMGW (i.e. intraSMGW) is mainly based on REST services supporting both XML and JSON data models;
- in order to improve the security, the communications services are based on certificates; on the interSMGW side the security is performed by means of the use of SOAP, on intraSMGW side the application of confidentiality and authentication mechanisms to REST services is based on use of HTTPS protocol by means of a public key X.509 certificate. In addition, the intraSMGW services are protected also by firewalling mechanisms;

This architecture promotes the management of security by using the SOA approach based on Web Services. It supports the use of SOAP and REST principles according to the features and nature of devices and services. In this scenario, the SMGW centralizes and manages all the communication and security issues. The security of the interSMGW services is managed by means of WS-Security

approach by using a message broker. The domain of devices contains heterogeneous communication technologies (and related security solutions) and the proposed model is designed to overcome the security problems in exchanging data over different domains.

1.3.4 Modelling techniques

Successful cyber-attacks against SCADA systems might put industrial production, environment integrity and human safety at risk. Within the CockpitCI project, abstract models, instantiated on an actual reference scenario, help to predict the consequences of such cyber-attacks with the goal of improving cyber security awareness of Critical Infrastructures. The actual reference scenario is composed of a SCADA system, its medium voltage electrical grid and a portion of a corporate network, which are an interdependent System of Systems and act as a whole to deliver electrical power to customers. Topologies, main functionalities, main devices and main communications among devices are included in the reference scenario.

Models have been built to predict the quality of electricity to customers of a Medium Voltage electrical grid, in case of cyber attacks to its SCADA, on the execution of FISR (Fault Isolation and System Restoration) procedure. On a permanent failure of the grid, SCADA operator executes FISR to locate, isolate and reconfigure quickly and safely the electrical grid. Anomalous operation of FISR, due to cyber attacks, may introduce longer delays in continuous supply of electricity and even cause the de-energisation of large part of grid customers. Cyber modelling is a relatively young domain and high fidelity models seem to require fine grain models which are relatively difficult to build. A general framework has been developed to model not only cyber-attack spreading but also the cyber-attack influence on the functioning of an electric infrastructure controlled by a vulnerable SCADA control centre over a vulnerable communication infrastructure. The modelling framework instantiates models which use different tools and formalisms:

- to model and analyze malware propagation in relation to the adopted SCADA & CCI security policies, NetLogo, a programmable modelling environment for simulating natural and social phenomena, has been used;
- to compute FISR performances as a consequence of Denial of Service (DoS) and Man In The Middle (MITM) attacks on specific SCADA & CCI devices, NS2, an open source tool for simulating communication networks and computing performances, has been used;
- to calculate QoS values, giving an indispensible information to estimate risk for final electrical customers, the RAO proprietary simulation model has been used.

1.3.5 Risk predictor

The Integrated Risk Predictor is a near real-time risk evaluation capability, which helps SCADA operators to better evaluate and react to potential threats, avoiding cascading effects, in line with existing service level agreements and availability levels contractually established with customers. The Integrated Risk Predictor, based on the interdependency analysis engine CISIA (Critical Infrastructure Simulation by Interdependent Agents), takes into account the presence of physical faults and cyber-attacks. Vulnerability assessment complements the risk prediction analysis and an incident response team is included in the loop to better manage the communication between operational teams (SCADA operators, IT operators) and the management level and to ensure coordination. The effect of countermeasures may also be assessed and previewed through simulation. Cyber propagation models are implemented in order to evaluate the holistic effects of an attack on the telecommunication infrastructure. Such effects, combined with the operativeness of TLC and SCADA elements, are then propagated in terms of service availability making use of interdependency models developed and tuned during the project.

1.3.6 Smart RTUs

In a typical CI architecture, the operational fault management is based on backup systems. Inactive during the system's normal operation, the backup systems become active if they detect isolation through heartbeat mechanisms. However, in case of cyber-attacks, such a system could be ineffective. To enhance the protection of CI architecture, the CockpitCI project has studied the deployment of smart agents at the lowest level (RTU) to cross-check information and actions. Deployed in clusters, these smart RTU or smart agents exhibit the following capabilities:

- The agent can estimate its own state and the local environment. This activity allows the agent to perform an assessment that is a pre-requisite for any autonomous decision.
- The agent can acquire information from its neighbours (cluster level decision) and/or receive commands/inputs from elements posed at higher hierarchical levels (system level decision).
- Each agent may assume that decisions at higher hierarchy levels are based on better situational awareness, and hence aims to prioritise these. However, due to the time latency to retrieve high level relevant information the agent is also able to identify the "right" actuation to be performed in case of risky situations.

The smart RTU concept is an innovative concept developed within CockpitCI which promises to distribute intelligence to the field and to open some kind of synergic cooperation between a local level of awareness and a global level of awareness. The CockpitCI project has developed a prototype of a smart RTU and has started to explore the potential benefits of this new concept.

1.3.7 Hybrid Test Bed

For the validation approach, the CockpitCI project uses the Hybrid Test Bed (HTB) based on the Hybrid Environment for Design and Validation (HEDVa) of the Industrial Control Systems (ICS) designed by the Israel Electrical Corporation Laboratory. The HEDVa is a distributed and virtualised environment that provides the possibility for remote and parallel operation of the different users locally or remotely. The HTB includes the part of the HEDVa customized to the requirements of the CockpitCI project and partners' labs integrated with the HEDVa. The HTB allows a mirror imaging of real critical infrastructures, to develop and test the tools and the methodology, to assess risk and simulate scenarios, and provides the following capabilities:

- simulation of operational levels (power grid, SCADA, Telco) according to real or simulated elements;
- collection and analysis of real traffic inside the HTB;
- provide test models and components for detection, identification, and mitigation of cyber-attacks on critical infrastructures;
- simulate cyber-attacks on different parts of CIs;
- identify and test vulnerable parts of CIs;
- test effectiveness of countermeasure plans, automatic reaction logics, the CockpitCI system functionality.

1.4 Potential impact, main dissemination activities and exploitation of the results

Potential Impact

The importance of Critical Infrastructures for modern society and their vulnerability has emerged clearly in the last 50 years. Several episodes have highlighted this vulnerability: in the 1960s the US blackout highlighted the fact that industrial infrastructures are vulnerable; in the 1990s an electrical outage in Italy due to telecommunication failure showed that the interdependency of Critical Infrastructure is a serious problem. Today, the emergence of sophisticated cyber-attacks shows that our technological societies are more vulnerable than we expected and ensuring security presents a new and primary societal challenge. The socio-economic impact of a failure of one or several Critical infrastructures can be extremely serious.

The CockpitCI has developed several concepts, techniques and devices, whose acceptance as a whole or partial according to one of several possible configurations, could represent a significant step forward in order to increase the reliability of Critical Infrastructures. One of the main results is the demonstration that the convergence among physical security, cyber security and business expectations especially in terms of QoS is possible with positive fallouts for all the involved players. Solutions like CockpitCI promote a Global Awareness to Improve CI Resilience and Dependability and this can be achieved through:

- Automatic detection and analysis of cyber threats;
- Near real-time prediction of operational risk for Critical Infrastructures;
- Sharing of near real-time relevant info among CI owners to maintain QoS;
- Use of a customised hybrid validation environment to test systems and strategies.

Benefits will arise from the security point of view thanks to the availability of a larger amount of field data, while, from the business point of view, a better near real-time risk evaluation will allow a tailored definition of service level agreement and the avoidance of large domino effects. The availability of such a technology will also foster some kind of cooperation among stakeholders; cooperation and sharing of information is in fact considered one of the most successful countermeasures to the cyber threat which is evolving in sophistication and in numbers at an unsustainable pace. The extent of such cooperation will gradually grow as confidence in the technology and trust among stakeholders grows.

CockpitCI is at the forefront of a new kind of systems, which are predictive rather than reactive. In the same way as we cannot exclude the occurrence of faults and natural events, it is not credible that we will always be able to keep the cyber attack outside of the perimeter of interest; breaches will occur sooner or later and we must be ready for it when it happens. An additional level of robustness is therefore needed which can:

- keep infrastructures in operation safely in adverse situations;
- maintain at least partial operational service rather than total shutdown.

CockpitCI aims to generate awareness over the entire System of Systems and to elaborate the near-term future in order to reduce any negative influence.

The potential impact of the CockpitCI project can therefore be summarized as follows:

- higher protection and resilience of Critical Infrastructures through the convergence of physical security, cyber security and business expectations;
- better risk assessment of the System of Systems by taking into account interdependencies;

- fostering increased cooperation among stakeholders;
- opening the way for next generation systems (aware, predictive, adaptive);
- addressing modern operational requirements thus increasing the competitiveness of system and technology providers;

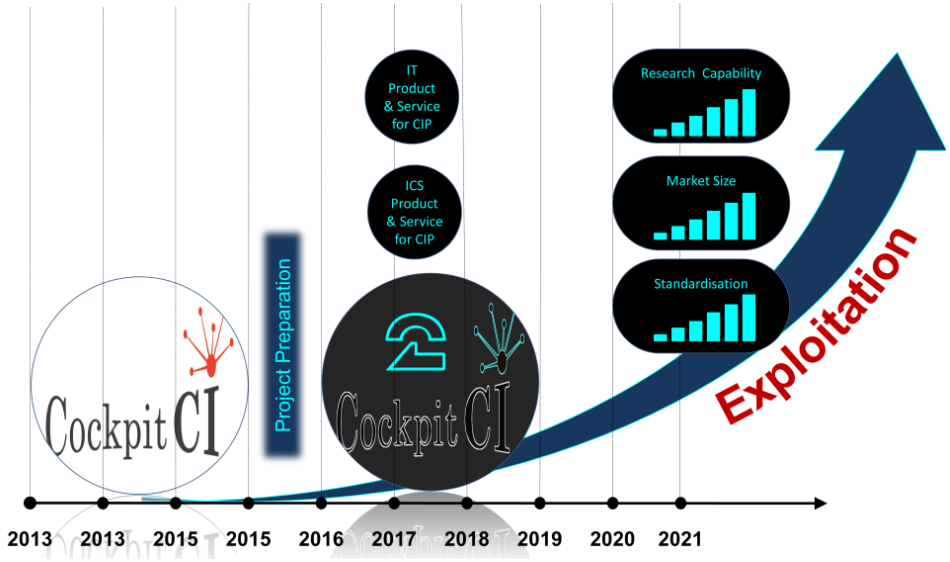
The potential impact of the CockpitCI system is not limited to the electrical domain but it applies to all types of Critical Infrastructures.

Main dissemination activities and exploitation of the results

Main dissemination activities include the production of more than thirty scientific papers, six dedicated workshops organized by the CockpitCI Consortium all around Europe and in Israel and the participation to the major event of CIGRE Congress 2014 in Brussel, where a stand was hired to demonstrate the first results and showcase the CockpitCI solution to potential end-users. The conference is the International Conference on “Innovation for Secure and Efficient Transmission Grids” organised by the CIGRE Belgian Nationale Committee and the AIM (Association des Ingénieurs de Montefiore) in Brussels on the 12th and 13th March and one of the most relevant event of its kind in 2014. The International CIGRE Congress has brought together more than 650 people from Electrical Technology Fields (production, distribution, protection) all over the world. A photograph taken during the exhibition of the CockpitCI stand is shown below.

The project idea and demonstrations have been welcome and deemed promising even if the cyber-threat is not yet recognized as a priority task for many industrial stakeholders and its operational challenge seems to be minimized in regard to the new technologies (especially smart grid, aero-cooling of the High Voltage cable, etc.). One of the major reservations formulated during the demonstration was about a real testing on concrete infrastructure. This reservation of course goes a bit beyond the scope of a research project but it was registered and served as an inspiration all the way through; the HTB and all its implications witness the great effort that was put in place by the Consortium to demonstrate the CockpitCI system on the real but of course not operational systems. However, according to the interviews and feedback on project deliverables, there is a very promising market for such products, especially due to failure of classical systems (such as IDS to protect SCADA systems) and the development of a commercial system based on the CockpitCI project could be a real success story.

According to these feedbacks, an exploitation plan has been designed. It is based on two major paths: i) the set-up of a “second phase” focused on the improvement of CI resilience, large scale validation and on assembling a “commercial” product based on the whole set of concepts, techniques and tools developed during the project. This product would provide incremental capabilities, starting with a basic solution that claims to be unobtrusive and transparent and which could quickly gain acceptance since it does not affect or minimally interrupt the normal operation of the infrastructure. This second phase could realistically be supported by a new project in the European H2020 framework; ii) the exploitation, which could start straightaway, of project knowledge acquired by each partner in their own environment to provide either services, consultancy or dedicated solutions.



1.5 Address of project public website and relevant contact details

For any reference please visit: http://www.cockpitci.eu