Cockpit CI

Cockpit CI

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

2012 2015

For more information

1 A. Bobbio, L. Egidi, E. Ciancamerla, M. Minichino, R. Terruggia, *Weighted attack trees for the cyber security analysis of SCADA systems*, DHSS, 2013 International Defense and Homeland Security Simulation Workshop 25 - 27 September, 2013, Athens, Greece

2 E. Ciancamerla, M. Minichino and S. Palmieri, *Modelling SCADA and corporate network of a medium voltage power grid under cyber attacks*, SECRYPT 2013,Iceland 29-31 July 2013

3 E. Ciancamerla, M. Minichino and S. Palmieri, *Modeling cyber attacks on a critical infrastructure scenario*, IISA2013, 10-12 July 2013

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

5 E. Ciancamerla, M. Minichino e S. Palmieri, *Cyber attacks spreading and impact on QoS of SCADA*, accepted to CRITIS 2012, 17 -18 Sept Lillehammer, Norway

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

7 A. Bobbio, A. Bonaventura, E. Ciancamerla, D. Lefevre, M. Minichino, R. Terruggia, *Temporal network reliability in perturbed scenarios: Application to a SCADA system*, In Proceedings IEEE Annual Reliability and Maintainability Symposium, pages 1–7, Reno, NV, 2012. ISSN : 0149-144X; ISBN: 978-1-4577-1849-6

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

9 S.L.P Yasakethu, J. Jiang, A. Graziano *Intelligent Risk Detection and Analysis Tools for Critical Infrastructure Protection*, IEEE Eurocon conference, Croatia, July 2013

10 M. Ouedraogo, M. Khodja and D. Khadraoui, *Predicting the QoS of Critical Infrastructures through Analysis of the Cyber Security Vulnerabilities*, ARES-RISI 2013 workshop

European Electrical Grid

To build the future together

The CockpitCI project aims to demonstrate 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.

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 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 cooperation among stakeholders; the extent of such cooperation will gradually grow as confidence in the technology and trust among stakeholders grows.

THE GRID MUST GO ON

Foreword

Selex ES

Project coordinator

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 the infrastructure. The CockpitCI project encompasses a multi-layered cyber detection framework capable of detecting anomalies or intrusion attempts on the entire critical infrastructure (CI) together with a near real-time risk evaluation capability which determines the CI functionalities impacted by cyber-attacks and faults, assesses the degradation of CI delivered services and supports the activation of possible containment strategies. CockpitCI provides the means for a smarter and more effective graceful degradation 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 tool (suited also for legacy systems) to a more sophisticated solution capable of limited automatic reactions in predetermined situations.

Project story

MICIE Cockpit CI

The protection of national infrastructures is one of the main issues for national and international security. The CockpitCI project stems from the previous FP7 MICIE (Tool for systemic risk analysis and secure mediation of data exchanged across linked CI information infrastructures) project, which has proved that by secure sharing of information on a near real-time basis among local risk predictors it is possible to increase the reliability and predictive capability of sensitive services. The final outcome is that operators receive information about the future evolution of their infrastructure with a wider perspective compared to previsions that can be generated by sector specific and isolated simulators.

Yet the MICIE approach is not enough in order to quickly and effectively react to all adverse events that may occur over the System of Systems and, in particular, to face cyber-attacks. In respect to cyber-attacks, CockpitCI aims to improve the resilience and dependability of Critical Infrastructures (CIs) through the automatic detection of cyber threats and the sharing of near real-time information about attacks among CI owners. CockpitCI aims to identify, in near real-time, the CI functionalities 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 and support the activation of a strategy of containment of the possible consequences of cyber-attacks. CockpitCI aims to leverage the ability of field equipment to counteract cyber-attacks by deploying preservation and shielding strategies able to guarantee the required safety. More specifically, the CockpitCI project has identified 6 main innovative approaches to enforce SCADA awareness:

- ☑ Integrated system
- ☑ Multi-layered Detection Framework
- ☑ Smart RTU
- ☑ Risk Predictor
- ☑ Risk Scenarios Modelling
- ☑ Hybrid Validation Approach

www.cockpitci.eu

in CSACI²P working group

FP7 European Research Project
Duration: 3 Years for 380 Person Months
Budget: 4.3 Mio€ funded at 3 Mio€

International Consortium of 8 countries
4 Universities 2 Research Centres
4 International Companies and 2 SME

Innovations

Integrated Solution

The first innovation of the CockpitCI project is the design of the solution, oriented to promote a close integration from cyber detection to risk prediction. The solution implements several adaptable services which can be embedded in 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 from 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 the use of RFC 4765 standard for detection message [IDMEF]) to be easily upgraded and integrated with already existing solutions.

Multi-Layered Detection Framework

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 (awaiting patenting) which promise to be effective also against Stuxnet-like threats..

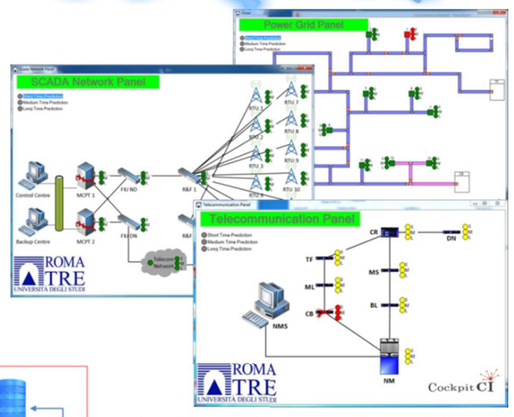
A near real-time risk evaluation capability, which is built on the cyber-awareness mechanisms helps SCADA operators to better evaluate and react to potential threats, avoiding cascading effects, in line with existing service level agreements and availability levels contractually established with customers. 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..

Smart RTU

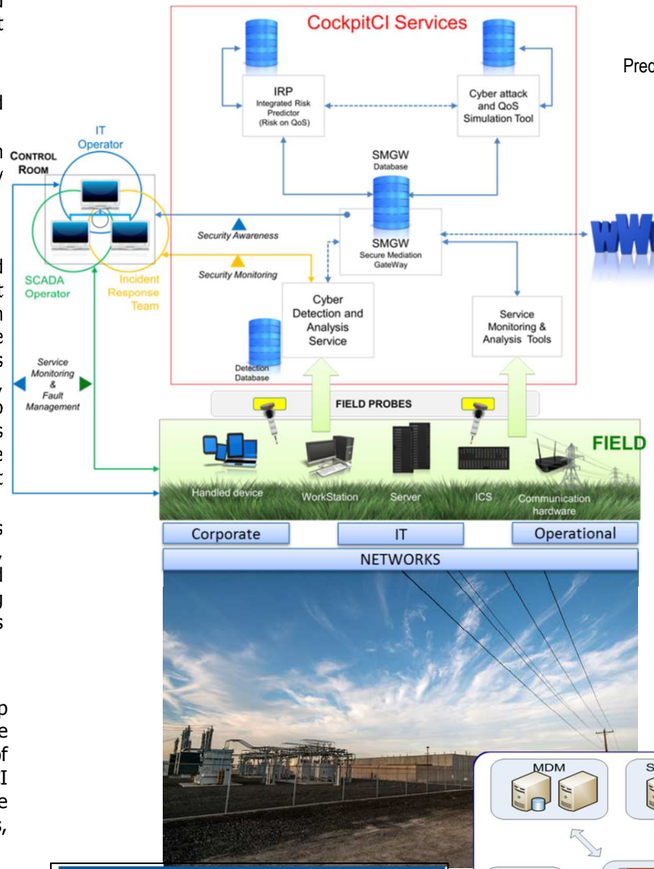
In a typical CI architecture, the operational fault management is based on backup systems. Inactive during the system's normal operation, the backup systems become active if they detect isolation through heartbeat mechanisms. However, in case of cyber-attacks, such a system could be ineffective. To enhance the protection of CI architecture, the CockpitCI project is studying 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:

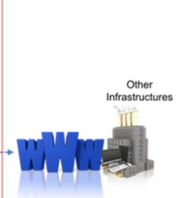
- ☑ The agent can estimate its own state and the local environment. This activity allows the agent to perform an assessment that is a pre-requisite for any autonomous decision
- ☑ The agent can acquire information from its neighbours (cluster level decision) and/or receive commands/inputs from elements 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 should hence aim 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 situation.

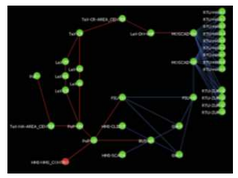
IEC Dispatching



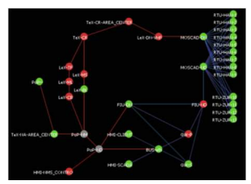
Prediction of the CI operational states by CISIA engine

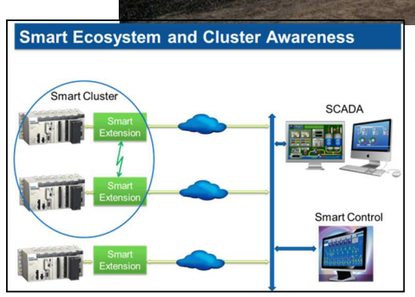


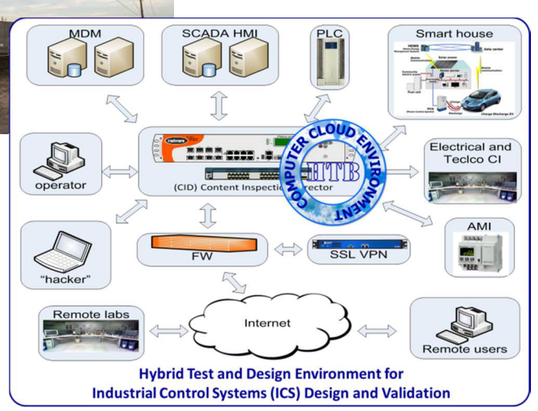




Modelling of virus spreading in CI architecture







Risk Prediction System

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 the 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.

Risk Scenario Modelling

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 in predicting 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.

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 is under investigation 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. Several heterogeneous models, software tools and their predictions within a reference scenario, are under investigation. Among them:

- ☑ agent based simulation (supported by RAO simulator);
- ☑ risk prediction by holistic reductionist approach;
- ☑ composed epidemic (NETLOGO simulator to model malware spreading) and performance models (open source NS2 to model DoS & MITM attacks).

Hybrid Validation Approach

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.