Reference no:

Hybrid Test Bed (HTB) & Tools for Cyber-attacks Simulation in SCADA Systems - CockpitCI Cybersecurity on SCADA: risk prediction, analysis and reaction tools for Critical Infrastructures Project

Dr. Leonid Lev Israel Electric Corporation Israel, Any Cohen - Israel Electric Corporation, Roman Tania Ecaterina, Program Director, IT & Telecommunications Division CNTEE Transelectrica SA; Voronca Simona-Lousie Deputy Chief Inspector, Systems and Critical Infrastructures Division CNTEE Transelectrica SA

CNTEE Transelectrica SA and Israel Electric are end-user partner in the *FP7 Project - Cyber-attacks against SCADA (Supervisory Control and Data Acquisition) systems* that are considered extremely dangerous for the CI's (Critical Infrastructure) cooperativeness and should be specifically addressed. Most of the cyber-attacks to ICS (Industrial Control Systems) are fake commands sent from the Control Centers to the RTUs (Remote Terminal Unit). CockpitCI intends to implement a comprehensive reliability and risk analysis tool for interdependent critical infrastructures, considering both intra-system and inter-system faults and risks models. Moreover, CockpitCI will develop comprehensive models integrating different events and cyber-attacks. The paper presents the benefits of using outcomes of the CockpitCI project in the critical infrastructures ICS operation (*http://www.cockpitci.eu*).

Keywords: cyber-security, critical infrastructures, test bed,

1. Scope and objectives

Protection of the national infrastructures (i.e. the System of Systems including energy grids, transportation networks, telecommunications systems, etc.) is one of the main issues of national and international security. US has established the (cf. CIP-002-009 [Cyber Security Standard]) of NERC - North American Electric Reliability). Europe has not deployed legal obligation on cyber security for Energy operators yet. Most of the ICS security requirements are specified by the CI operators, relying on the ISO (International Standards Organization) 27001 approaches, other standards or even their own goods practices.

The family of standard 270xx allows to assess the security of the information system and gives guidelines to apply good security practices (ISO 27002) and to improve the security in several domains as Incident Management (ISO 27035), Business Continuity (ISO 27031), cyber security (ISO 27032), and network security (ISO 27033).

Some more specific standards for ICS security are provided in the US by ISA, e.g. ISA-99.00.02, "Security for industrial automation and control systems", establishing an industrial automation and control systems security program. Those standards are currently changed into the 62443 international standard IEC (International Electro-technical Commission).

.

2. Consortium

The consortium of the project includes 12 partners from 8 different countries, 7 from Europe (Italy, Belgium, Portugal, Luxembourg, UK, Romania, and Norway) and one from Israel. The consortium integrates all the appropriate key players to ensure the availability of technologies, capabilities, technical and operational knowledge required for the success of the project. SELEX Sistemi Integrati from Italy the coordination of the project, Reserche Public Henri Tudor from Luxembourg, Consortium for Research in Automation and Telecommunication University of Rome – „La Sapienza" from Italy, Dipartimento Informatica e Automazione – Universita degli Studi Roma TRE from Italy, Agenzia nazionale per le nuove technologie, l'energia e lo sviluppo economico sostenibile from Italy, Israel Electric Corporation from Israel (IEC), ITRUST Consulting SRL from Luxembourg, Multiasbl from Belgia, University of Colimbra, Faculdade de Ciencias e Tecnologia from Portugal, Surrey University from UK, Lyse Energy from Norway and C.N.T.E.E. Transelectrica SA.

3. Work Packages

The project is managed according to the contract between the CockpitCI Consortium and the European Commission.

The main objective of the CockpitCI project is to increase the resilience of SCADA systems in presence of cyber-attacks by provide an integrated solution for protection of ICS against cyber-attacks

The project contributes to the following fields of critical infrastructure protection research:

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

4. Hybrid Test Bed (HTB)

For the Cockpit CI tool validation, 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 partner's 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; simulation of 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.

The role of the HTB in CockpitCI project is to support CockpitCI tool development and validate defence models for different types of ICS with the following capabilities:

- 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;
- Easy remote access to test environment;
- Simulate separate logical test environments;
- Saving logical test environments for reuse in future.

CockpitCI HTB includes the following components:

- Electrical and telecom equipment;
- Virtual machine infrastructure;
- Test-environment network-flow management infrastructure;
- SCADA management systems
- Telecom management system;
- Electrical infrastructure simulator;
- Elements of network infrastructure (SDH, Cellular, VHF).

The HTB includes procedures, historical data SCADA HMI and RTUs that enable the supervisor in the control centre to receive alarms of electrical grid faults and RTUs operation, electrical grid fault location, isolation and service (reenergize) restoration.. All actions are performed remotely by open and close switches simulated by PLCs (Programming Logical Controllers). Distribution Management System Control Centre is based on the SCADA HMI Cimplicity that enables to execute remote command and control operations based on equipment, historical data and procedure simulators of the HTB. The HTB concept view is presented in Figure 1 [1].

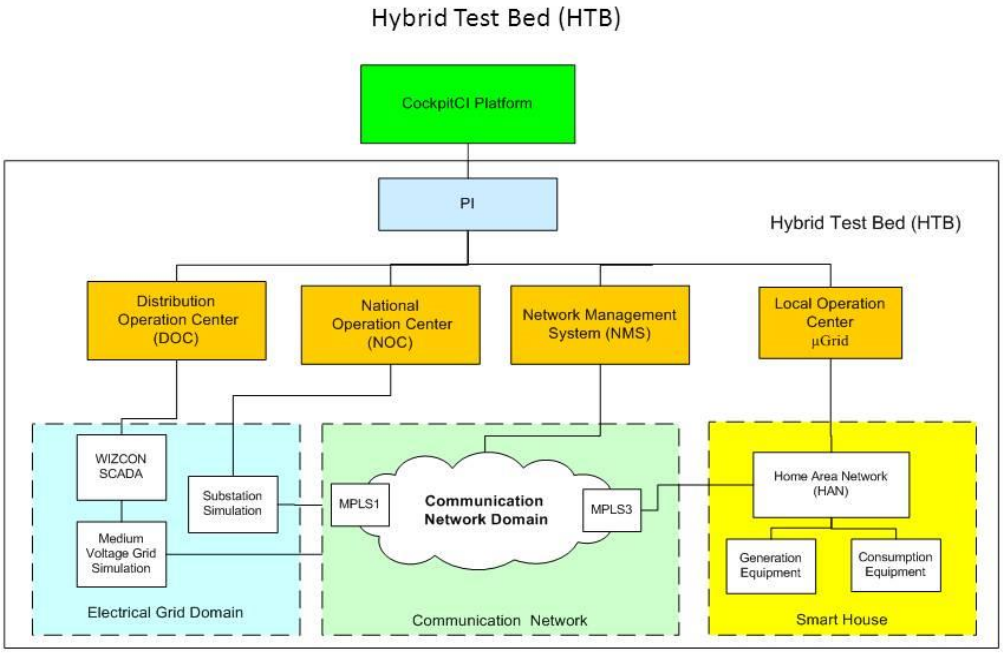

Figure 1. Hybrid Test Bed concept

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 is connected to network-flow management infrastructure that includes the following components [1]:

- Content Inspection Director (CID) is a core element of network-flow management infrastructure. CID manages logically defined network-flow redirection through:
  - 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 test-environment components (servers, work stations, SCADA applications, etc.) is managed by SSL (Secure Sockets Layer) VPN appliances.

- The components of the test-environment installed on remote sites of CockpitCI partners, could be connected to HTB test-environment through VPN (Virtual private Network) channels based on FW-FW IPSEC (Internet Protocol Security) VPN.

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

- Aggregation of remote labs from Roma3 and Coimbra universities to the CockpitCI Validation system,
- Implementation of the bidirectional remote access to all resources of the CockpitCI Validation system,
- CockpitCI system and HTB aggregation in the CockpitCI Validation system,
- Development of the verification and validation scenarios for CockpitCI system,

CockpitCI customized HTB configuration is presented in the Figure 2.[1]

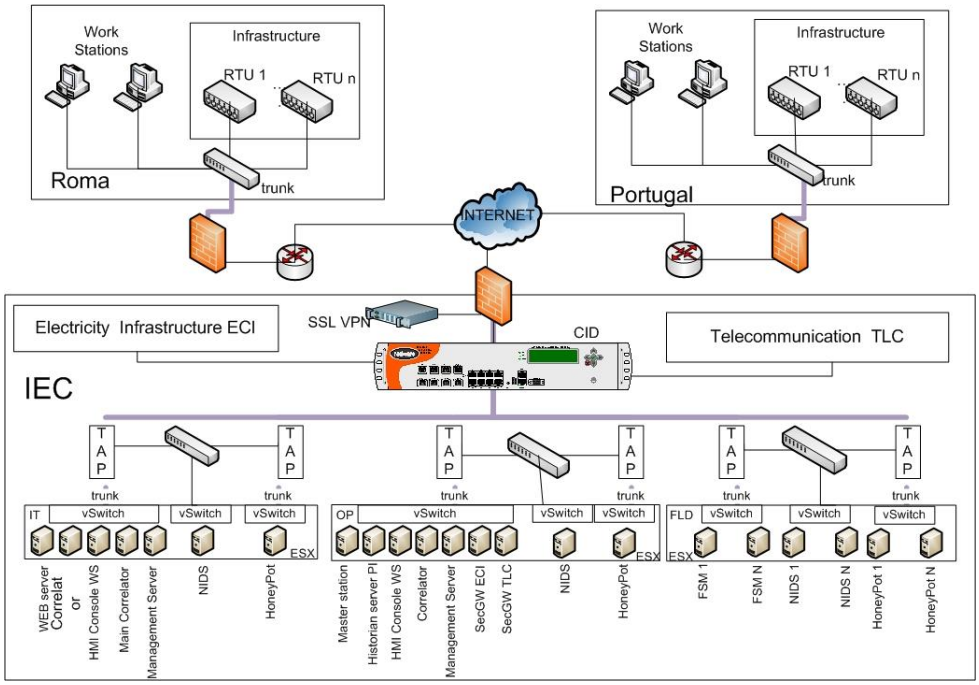

Figure 2. CockpitCI customized HTB configuration

Examples of cyber-attacks goals [1]:

- Attacker sends inaccurate/false information to system 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 operators to prevent them from being aware of conditions or to initiate inappropriate actions.
- Overtaxing staff resources due to simultaneous failures of multiple systems.

5. Conclusions

ICSs are always susceptible to cyber-attacks. Different types of cyber-attacks could occur depending on the architecture and configurations used in the ICS. These attacks specified by the following four categories [2]:

- Internal/Non-malicious - employees or contractors causing unintentional damage;
- Internal/Malicious - system users with extensive internal knowledge of the system who intentionally cause damage;
- External/Opportunistic - hackers seeking a challenge;
- External/Deliberate - malicious, well-funded political activists, organized crime groups, or nation states.

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

The CockpitCI tool validation scenarios implementation will ensure that the tools' functions will be implemented as required, including operational behaviour and user interface. The hardware and the software will be validated at the system integration level. This step is beyond the software and hardware verification processes.. CockpitCI validation will be performed by an independent IEC team and will be performed in the system validation environment.

Reference

[1]Cyber-security on SCADA: risk prediction, analysis and reaction tools for Critical Infrastructures Task 6001 Validation plan and scenarios design and implementation L. Lev, D. Tanenbaum, L. Rozenblum, O. BenArush

[2]Deliverable of the project - D5.2- CockpitCI System architecture design, Antonio Graziano, Pietro Ricci-Selex Integrati, Donato Macone, Francesco Liberati, Andrea Simeoni – CRAT, Lasith Yasakethu – Surrey University, Matthieu Aubigny –ITRUST, Stefano Panzieri –TRE Roma University.[2012]