EMERGING INFORMATION TECHNOLOGY SCENARIOS FOR THE CONTROL AND MANAGEMENT OF THE DISTRIBUTION GRID

Giovanna DONDOSSOLA
CESI RICERCA – Italy
dondossola@cesiricerca.it

Fabrizio GARRONE
CESI RICERCA – Italy
garrone@cesiricerca.it

Judit SZANTO
Consultant – Italy
szanto@cesiricerca.it

Gennaro FIORENZA
ENEL Distribuzione – Italy
gennaro.fiorenza@enel.it

ABSTRACT

This papers presents a set of scenarios highlighting critical aspects related to the role of Information Technology in the management of the Distribution Grid. The case study has been developed inside the "CRitical UTility InfrastructurAL resilience (CRUTIAL)" European project.

INTRODUCTION

Today's Electric Power Systems (EPSs) are undergoing a strong renewal process, based on an increasing trend to rely on the concepts of remote supervision and control, interconnection of power structures and online power system monitoring. Communication networks are extensively used by technically advanced power utilities to support both real time and non real time information exchange with obvious benefits, thus assuming a major role in power system management. Due to the intensive use of information and communication systems, which are exposed to a vast amount of accidental and intentional cyber threats, cyber security has become a relevant issue for utilities managing critical infrastructures. The identification of critical aspects of control system architectures as a subject of technological solution studies, is one of the objectives of the European Project CRUTIAL [1].

As a first step towards the achievements of the CRUTIAL objective, the paper presents a subset of the scenarios developed within the project [2], addressing both concrete needs and envisaged evolutions, related to the Distribution Grid's control system. The selected scenarios have been conceived in view of a full integration in the operation and control infrastructures of the Power System, i.e. Generation, Transmission and Distribution, and of the development of a global national defence plan involving the different stakeholders. The scenarios cover emerging themes like information and communication security aspects of power substation control, support to emergency management by the distribution grid control, interactions between process control and corporate activities and remote maintenance of ICT automation devices.

Our case studies focus on intentional threat hypotheses [3] [4], having either exogen (external) or endogen (internal) source, such as Denial of Service (DoS) attacks to remote control communications; intrusions into Centre-Substation communication flow and execution of faked commands; exploitation of vulnerabilities of the standard application layer protocols; viral infections of the Substation Control Network caused by malicious maintenance activities.

Significant aspects of the scenarios shall be investigated on a laboratory testbed reproducing the essential features of a reference architecture consisting mainly in a generic distribution network control system and a restricted set of interacting Transmission/Distribution components.

Section 2 of this paper describes the CESI RICERCA laboratory platform used for the testing and demonstration of the control system scenarios and the reference architecture the testbed is based on; section 3 illustrates key aspects of the scenarios under development, and section 4 concludes the paper.

LABORATORY TESTBED AND REFERENCE ARCHITECTURE DESCRIPTION

The laboratory testbed is based on the distribution network section of the Power Control System and shall be used to:

- identify the critical aspects of the interdependency between Power and ICT systems,
- highlight the ICT system's vulnerability to potential cyber attacks and
- evaluate the resiliency of possible architectures/ mechanisms/ solutions to cyber threats.

Reference architecture

Focusing on the ICT/communication aspects of the EPS, this may be seen as a set of interconnected nodes consisting of Substation Control Systems and related high level Control Centres (Transmission System Operator (TSO)s', Distribution System Operator(DSO)s', Generation Company (GENCO)s', Power Exchange's, Energy Authority's, etc.) involved in the electrical system's management (see Figure 1).

There are basically two kinds of information flow over the communication network:

- real time communication between grid control centres (supervisory control and data acquisition (SCADA) systems and energy management systems (EMS)) and substation control systems;
- non real time communications directed to back office departments for the transmission of data (e.g. statistics, trends, condition related data) to be used for protection engineering, maintenance, planning and asset management, etc.

Consequently, the communication system itself consists of a set of interconnected network segments each with its own performance requirements, with extensive use of open and shared, or even fully public, networks. Both DSOs and

TSOs rely, for instance, on maintenance services from external providers, who mostly use public communication networks to receive timely status information about the equipment to be maintained.
A Centralised Control Centre provides monitoring and management functions for the whole ICT infrastructure (communication networks, Intelligent Electronic Devices-IEDs, etc.).

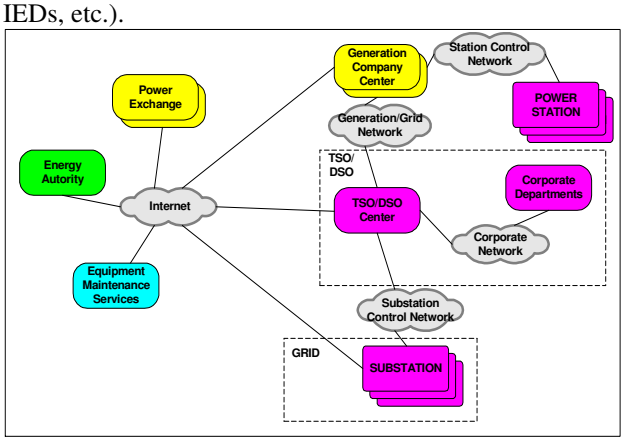

Figure 1 : Information flow in the EPS

The reference architecture for our testbed (see Figure 2) is a generic distribution network control system using standard Telecom IP backbones for Centre-Substation communications.

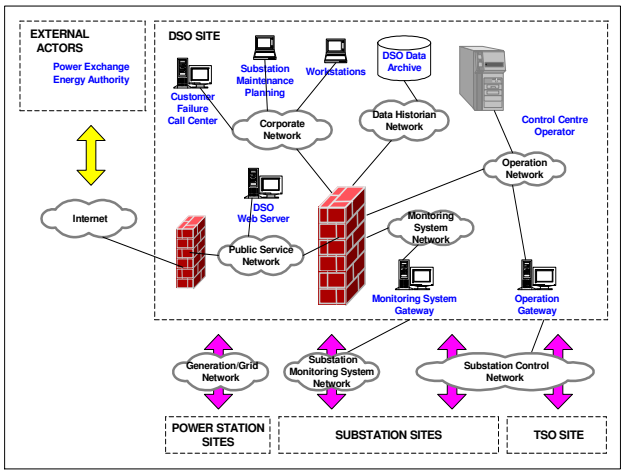

Figure 2: Example of Distribution Power Grid Section

Reference Communication Scheme

The following assumptions apply to inter site communications:

- at the application level, communications among Control Centres comply with the standard IEC 60870-6 [7] *Inter-Control Centre Communications Protocol* (ICCP/TASE-2), while Centre-Substation communications are based on the IEC 60870-5-104 standard [6]. Both protocols are IP based and they mostly rely on a connection oriented transport layer (TASE-2 uses MMS-Manufacturing Message Specification, ISO 9506), although UDP/IP may also be used for multicast datagram transmission;
- the datalink level consists of standard Telecom IP backbones (owned by independent telecommunication service providers), with redundant communication paths, implemented over physically independent carrier lines, granting the system's availability requirements in case of accidental failures of ICT components.

Testbed Architecture

The laboratory testbed, which is being designed by CESI RICERCA for the CRUTIAL project [5], implements a prototypal but significant power system management architecture with its integrated ICT infrastructure.
Focus is being placed on the development of those aspects of the actual Power Control System which can be used for the implementation of a set of significant attack scenarios, in order to evaluate their feasibility and plausibility, to demonstrate the possible evolution of the attack processes and to assess the severity of the potential damage on the attack's target.
The CESI RICERCA testbed's architecture shall be a strongly simplified version of the reference Power Grid architecture on which it is being modelled. As the main purpose of the laboratory testbed consists in the evaluation of the cyber security issues related to the Power Grid infrastructure, the prototype shall be designed according to the following guidelines:

- all those components of the reference architecture which can be involved in the cyber attack scenarios to be demonstrated shall be modelled as faithfully as possible;
- the implementation of the other components shall instrumental to the demonstration i.e. shall be a simplified representation of the actual control system components.

At the present preliminary phase of the development, the testbed includes two primary substations, controlled by a simplified remote Distribution Control Centre and a Monitoring Control and Defence Terminal Unit (MCD-TU) of the transmission control system.
The testbed's communication architecture, based on the reference communication scheme is being designed according to the same criteria followed in modelling the automation sites: all those aspects which are not considered significant with respect to the proposed attack scenarios are strongly simplified. The assumptions are the following:

- the two lower layers of the OSI stack (physical and datalink) are modelled by switched Ethernet, both for local and wide area communications;
- TCP/IP and UDP/IP shall be used at the transport layer;
- application layer data exchange shall not make use of commercial protocols, but the contents of the application Protocol Data Units (APDU)s shall be compliant with the appropriate standard.

CONTROL SCENARIOS

By CONTROL SYSTEM SCENARIO we mean a reference structure and behaviour of (a portion of) the Power System, the related Monitoring, Control and Maintenance Networks and devices, including communication, host and server devices, in a hostile environment exposed to threats that may jeopardise the operation of the power system services. The Control System Scenarios explored in CRUTIAL are derived from state of art power control systems and their envisioned evolution with the main purpose to assess the capacity of the communication architecture to tolerate the most common threat hypotheses, evaluating:

- the security of the communications in the supervision and control systems of grid and generation operators;
- the impact of attacks in emergency conditions;
- the possible breaches caused by interactions between the corporate and the process network;
- possible problems related to the ICT system's remote maintenance.

In the following paragraph we shall discuss four possible scenarios, related to the aforementioned issues.

Security of remote teleoperation and control functions for grid operators

The purpose of this first scenario is to evaluate the information and communication security of a MV DSO. As already mentioned the information flow between Area Control Centres and their supervised Substations is supported by standard Telecom IP backbones owned and operated by an external provider who supplies a virtual, dedicated channel over a communication link shared with other customers. The inter-site communication infrastructure may be assimilated to a public WAN.

Due to the strong availability requirements on the communication system (availability 0.99999), it is supposed that redundant communication paths are used, implemented over physically independent line carriers, eventually owned by distinct Telecommunication providers.

The purpose of this scenario is to assess the capability of the redundant communication architecture to tolerate the threat hypotheses and evaluate the possible cascading effects in presence of power contingencies (insufficient production, generation trip or HV line unavailability).

ICT threats that may affect the communication infrastructure range from DoS attacks to the telecontrol operations and intrusions into the Centre/Substation communication flow eventually followed by the execution of faked commands, to the exploitation of the vulnerabilities of the standard application layer protocols used for monitoring activities and commands transmission.

Interaction between grid operators in emergency conditions

This scenario explores the security of the communications between the Transmission and Distribution System Operators under emergency operating conditions (i.e. under-frequency or voltage instability), assessing the possible cascading effects of ICT threats to the communication channels connecting TSO and DSO Control Centres and Substation Monitoring Control and Defence Terminal Units (MCD-TUs).

It is assumed that in emergency conditions the TSO is authorised by the DSO to activate defence plan actions, consisting in the performance of load shedding activities on the distribution grid.

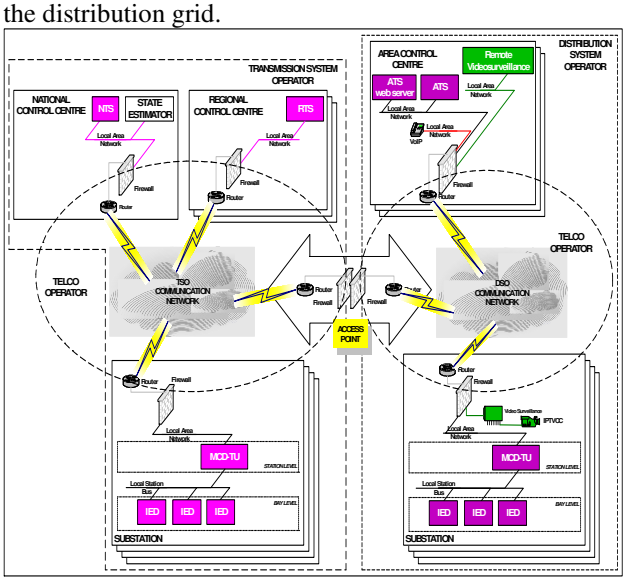

Figure 3: TSO and DSO telecontrol systems

As visualised in the Figure 3 all the telecontrol systems of TSO and DSO are involved in this scenario. Cyber attacks carried out under emergency conditions, when defence actions have to be performed out under strict real time constraints, can cause severe damages, like inhibiting the required automatic load shedding actions.

Integration between process control and corporate activities

This scenario explores the integration of process control and corporate networks in a MV DSO Control Centre, evaluating the possible cascading effects of cyber attacks on the integrated architecture. Access to process information is granted to a variety of Corporate functions (administrative, management, maintenance, metering, etc.), by means of the DSO intranet. Communications are filtered by a central firewall.

The information exchange between the actors includes measurements, signals, metering data, etc. and information flow is supported by IP based standard protocols providing the following services:

- Web Services in case of web applications (e.g. http);
- SQL queries to access the Data Base;
- Data Exchange (e.g. ftp).

The purpose of this scenario is to assess the vulnerability of the central firewall in the Control Centre, the resilience of

the most critical process control applications and the possibility of compromising process data.
The following ICT threats are under consideration:

- Viral infections propagating from the Corporate Network to the Process Network;
- Vulnerabilities of standard application layer protocols (ex. http and ftp) used for power management related communications;
- Intrusions into the databases of the Area Telecontrol and Metering systems and corruption of process data.
- The occurrence of the considered ICT threats may cause the reduction of the DSO communication bandwith with degradation in SCADA response time and possible cascading phenomena as in the first scenario and the unavailability or wrong perception of essential data with possibly severe consequences as for instance economic losses due to wrong.

Remote ICT Maintenance for grid operators

This scenario assumes the presence of a centralized ICT maintenance service with a Central Control Centre for the monitoring and control of the ICT assets in the DSO control system. The ICT maintenance service performs:
This scenario considers the use of a centralized ICT maintenance service assuming the presence of a central Control Centre for the monitoring and control of the components of all the ICT assets in the DSO process network providing:

- remote ordinary maintenance activities on the ICT components;
- continuous monitoring of the ICT equipment status, including security monitoring functions;
- repair actions on ICT network and equipment configurations.

The information flow interesting maintenance activities includes the transmission of status information towards the Control Centre and the delivery of commands and data related to functional testing and remote operation of ICT devices (e.g. runtime reconfiguration) from the Centre. There are no real time requirements.
The remote maintenance system relies strongly on the internet and is exposed to all possible cyber threats affecting ICT components (e.g. IEDs, Routers, Servers, Firewalls).
The severity of the damage caused by the cyber attacks depends of course on the number of components affected and on their role in the operator's services, with cascading effects having as ultimate consequence the loss of the supervision and monitoring maintenance functions.

CONCLUSIONS

The concept of control system scenario resulted in a useful starting point for the discussion on the interdependencies of power and ICT infrastructures during the first year of the CRUTIAL project. The scenarios described in the paper may offer the scientific and technical community some important issues to be addressed by future power control systems and guidelines towards the deployment and development of architectural and technological solutions.

Acknowledgments

This work has been partially financed by the Ministry of Economic Development with the Research Fund for the Italian Electrical System under the Contract Agreement established with the Ministry Decree of March 23, 2006. It is also partially supported by the European Commission with the Project IST-4-27513 CRUTIAL participated by several institutions: CESI RICERCA (Italy), FCUL (Portugal), CNR-ISTI (Italy), LAAS-CNRS (France), K.U.Leuven-ELECTA (Belgium), CNIT (Italy) http://crutial.cesiricerca.it/.

REFERENCES

[1] G. Dondossola, G. Deconick, F.Di Giandomanico, S. Donatelli, M. Kaâniche and P. Verissimo, 2006, "Critical Utility Infrastructural Resilience", *Proc. Int. Workshop on Complex Network and Infrastructure Protection,* CNIP 2006, 28-29 March Rome, Italy, 183-195.

[2] CRUTIAL Project, 2007, *Analysis of new control* applications, Deliverable D2.

[3] G. Dondossola, O. Lamquet and A. Torkilseng, 2006, "Key issues and related methodologies in the security risk analysis and evaluation of electric power control systems", in *7*, Study Committee D2 "Information, Telecommunication and Telecontrol systems in the Electric Power Industry", Paris, France.

[4] G. Dondossola, J. Szanto, M. Masera and I. Nai Fovino, 2006, "Evaluation of the effects of intentional threats to power substation control systems", *Proc. Int. Workshop on Complex Network and Infrastructure Protection,* CNIP 2006, 28-29 March Rome, Italy, 309-320.

[5] CRUTIAL Project, 2007, *Testbeds deployment of representative control* algorithms - Interim Report, Deliverable D24.

[6] IEC 60870-5 Telecontrol equipment and systems – Part 5-104: *Transmission protocols – Network access for IEC 60870-5-101 using standard transport profiles*, International Standard, Second Edition, Reference Number IEC 60870-5-104 (E).

[7] IEC 60870-6 *Telecontrol equipment and systems – Part 6-503: Telecontrol protocols compatible with ISO standards and ITU-T recommendations – TASE.2 Service and protocol*, International Standard, Second Edition, Reference Number IEC 60870-6-503 (E).