THE SINARI PROJECT: SECURITY ANALYSIS AND RISK ASSESSMENT APPLIED TO THE ELECTRICAL DISTRIBUTION NETWORK

John MCDONALD
Helene DECROIX
EDF R&D – France
John.McDonald@edf.fr
Helene.Decroix@edf.fr

Raphael CAIRE
Jose SANCHEZ
G2ELabs – France
raphael.caire@g2elab.grenoble-inp.fr
jose.sanchez@g2elab.grenoble-inp.fr

Stephanie CHOLLET
ESISAR – France
Stephanie.Chollet@lcis.grenoble-inp.fr

Nouha OUALHA
Armand PUCCETTI
CEA LIST – France
nouha.oualha@cea.fr
armand.puccetti@cea.fr

Artur HECKER
Claude CHAUDET
Telecom Paris Tech – France
artur.hecker@enst.fr
Claude.Chaudet@enst.fr

Henri PIAT
Daniel GEORGES
Atos WorldGrid – France
henri.piat@atos.net
Daniel.georges@atos.net

Frederic PLANCHON
FP Conseil – France
frederic.planchon@wanadoo.fr

ABSTRACT

This paper presents a summary of the key results obtained within the "SINARI" project; a French collaborative research project which focuses on developing methods for assessing the dependability and cyber security of the coupled infrastructure made up by the electrical distribution network and its supporting information system and telecommunication infrastructures. This paper will present an overview of the project as a whole and will summarize the work already completed along within highlighting the ongoing activities.

INTRODUCTION

The electric distribution network is undergoing a period of profound evolution. From a passive distribution network with limited monitoring, the network is evolving towards an increasingly active, "smarter", highly monitored network. At the heart of this evolution is an increased use of Information and Communication Technologies (ICT). ICT will play an important role in enhancing and improving the performance of existing network functionalities while also enabling potentially new functionalities.

The increasing presence of ICT can only heighten the interdependency and the complexity of interactions between the electrical distribution network and the associated information systems infrastructure and telecommunication infrastructure. An increased exposure of any of these coupled infrastructures to coincidental failures (i.e. reliability issues) or mischievous/malicious activities (i.e. security issues) represents a point of concern.

This concern is underscored by the number of international working groups (e.g. CIGRÉ D2.22 [1] and D2.31 [2]), and recently completed or ongoing European research projects (such as CRUTIAL – "CRitical UTility InfrastructurAL Resilience" http://crutial.rse-web.it/, VIKING – "Vital Infrastructure, NetworKs, INformation and Control Systems ManaGement" http://www.vikingproject.eu, SESAME – "Securing the European Electricity Supply Against Malicious and Accidental Threats" http://www.polito.it/sesame/) who all address aspects of this issue.

Added to this list is the "SINARI" project (www.sinari.org); a collaborative research project sponsored by the French National Research Agency (ANR). The SINARI project – "Security of Infrastructures and Analysis of Risks" (www.sinari.org) is focused on the assessment of the impact of ICT mal-performance on the safe and reliable operation of the electrical distribution network along with the development of operational models of the interdependent infrastructure that will aid the securisation of the functions, equipments and systems within the coupled electrical distribution networks – ICT infrastructures.

This paper will present an overview of the project and the work already completed along within highlighting the ongoing activities. Focus will be given to:

- the selection and/or development of methods for the modelisation of the interdependent infrastructures;
- the examination of risk analysis methods and their subsequent application to an aspect of electrical distribution network performance; and
- the conception and on-going development of physical platform which will be used to evaluate the effectiveness of certain countermeasures.

PROJECT STRUCTURE

Launched in 2010 and currently in its final stages, the SINARI project brings together six partners (Atos WorldGrid, CEA LIST, EDF R&D, FP Conseil, INP G2ELab, Telecom Paris Tech) to develop methods for assessing the dependability and cyber security of electricity distribution network. Likewise the project aims to identify effective and necessary countermeasures for these interdependent electrical distribution networks – ICT infrastructures.

The project has focused on the behavior of the substations linking the transmission and distribution systems (an element of the electrical distribution network whose performance already includes a reliance on ICT systems) and the associated medium voltage distribution network.

The key elements of the project include:

- Identifying the hazards and risks inherent in the coupled electricity distribution networks, information infrastructures and telecommunication networks,
- Developing the effective and necessary defences/countermeasures for the ICT systems for the electrical distribution networks,
- Testing and evaluating, using a physical platform, some representative defence schemes and countermeasures.

The work structure of the project is shown in Figure 1.

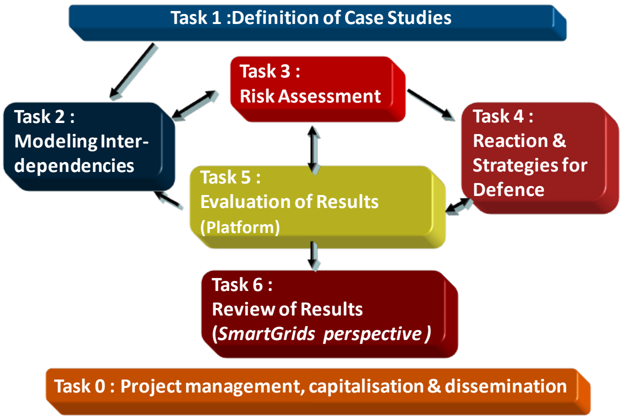
Task 1 :Definition of Case Studies
Task 2 : Modeling Inter-dependencies
Task 3 : Risk Assessment
Task 4 : Reaction & Strategies for Defence
Task 5 : Evaluation of Results (Platform)
Task 6 : Review of Results (SmartGrids perspective)
Task 0 : Project management, capitalisation & dissemination

Figure 1 Work structure of the SINARI project

It should be highlighted that the SINARI project focuses on the behaviour of the existing electrical distribution network, rather than a future "smarter" distribution network. The following discussion will give an overview of the nature of the work carried out in the key tasks 2, 3 and 5.

MODELISATION OF INTERDEPENDANT SYSTEMS

An inherent difficulty associated with assessing the importance of ICT mal-performances is the absence of appropriate theoretical tools for modelling the behaviour of interacting infrastructures. A key task within the SINARI project has been then the examination of the relative merits of a range of different technique for modelling interacting systems. The techniques examined included: Agent based modelling; Petri nets; co-simulation methods; complex network analysis and Boolean logic Driven Markov Processes (BDMP). The results of this comparison have been captured in a previously published work [3]. The following discussion focuses on the two techniques of "co-simulation" and "complex network analysis" which have been given the most attention within the project.

Co-simulation

Co-simulation or cooperative simulation represents a process where the behaviour of interacting systems are simulated using dedicated simulation tools for each of the different systems and developing a framework or mechanism to handle the interactions between the different tools. This approach represents an extension of the single infrastructure simulation techniques that have been commonly used to date to assess the performance of electrical network.

There are two main challenges in applying this approach. The development of the unified simulation environment is a non-trivial task, given that dedicated commercial packages are not yet available. Added to this, the selection of appropriate parameters for representing credible scenarios within the simulation environment remains an ongoing task.

Complex Networks

A more theoretical approach being pursued is the use of the "Complex Networks" analysis techniques as a means of representing the elements and interactions of the different interdependent infrastructures (e.g. electrical distribution network - ICT systems). By developing a graph based representation of the interacting infrastructures, it is possible to treat both random failures (i.e. reliability) and the "deliberate" failures (i.e. ICT security) in a more unified fashion. In this way it is possible to describe the structure of the interdependent systems and thus potentially identify vulnerabilities of the overall systems.

The application of these techniques to characterise the performance of the electrical power systems represents a point of ongoing research and it is expected the final result of the SINARI project will contribute further to this field.

RISK ANALYSIS

Clearly, although techniques for better modelling interdependent infrastructure are being developed, it is still important that we can analyse the inherent risk associated. This is particularly important for the practical case of the use of ICT to support the operation of an electrical distribution network. At present, however, there is still a lack of clarity regarding the relative merits of the different risk assessment methods that can be applied to this problem.

An extensive review was undertaken to identify suitable methods. The review covered a range of standards, methods, and "best practices" for ICT security as proposed by national and international organizations such as ISO (International Organization for Standardization) or the French ANSSI (National Security Agency for Information Systems). The approaches considered included ISO / IEC 27005, SP 800-30 [4] and IEC 61508 [5] as well as the methods: EBIOS [6], MEHARI [7 - 8], CRAMM [9], and SQUARE [10].

Following this comparison, the technique EBIOS was selected. EBIOS (Expression des Besoins et Identification des Objectifs de Sécurité)1 is a comprehensive technique

[1] The phrase « Expression des Besoins et Identification des Objectifs de Sécurité » translates to « Expressions of Needs and the Identification of Objectives of Security ».

dedicated to Information System risk assessment, originally developed by the French government. The technique can be adapted to different contexts and is capable of treating aspects of ICT reliability as well as ICT security. In addition, it makes use of a notion of risk more general than methods solely on the propagation of dysfunctions (such as FMEA2 or HAZOP3). Finally, it also permits a "nested" approach to risk assessment where more complex, domain specific techniques can be integrated within the overall analysis framework to improve the robustness of the risk assessment.

EBIOS

As illustrated in Figure 2, EBIOS consists of 5 phases. Phase 1 deals with an analysis of context in terms of global business process dependency on the information system. Both the security needs analysis and threats analysis are conducted in phases 2 and 3, yielding a vision of their conflicting nature. In phases 4 and 5, this conflict, once arbitrated through a traceable reasoning, yields an objective diagnostic on risks. Further steps may be required if the technique is to be used for risk management rather than just risk assessment.

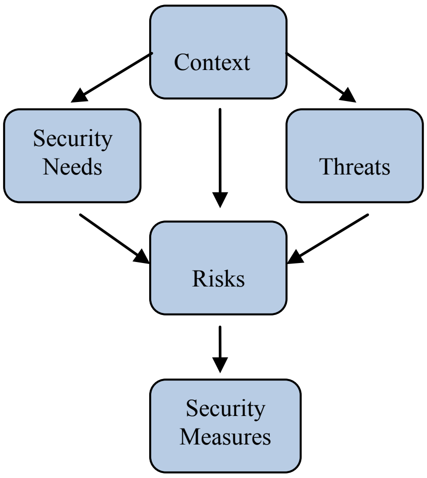

Figure 2 Structure of risk analyse technique "EBIOS"

In the case of the electrical distribution substation, EBIOS has been used to assess the relative importance of the different interfaces and information exchanges within the substation's ICT system. Likewise, certain failure modes which pose greater potential hazards have been identified. Although the results obtained remained essentially qualitative rather than quantitative, the technique represents a valid approach for comparing design and operational choices, such as, for example, different ICT architectures or the use of different security policies.

That said, the essentially qualitative nature of the technique does remain a limitation. An accurate representation of the inter-dependence between the ICT system and the supported distribution network remains a challenge. Likewise, the treatment of the dynamic aspects of ICT use in electrical distribution substations (including the impacts of changing topologies and operating regimes of the electrical distribution network) remains an area of ongoing work.

DEMONSTRATOR

The techniques described in the preceding sections are essentially theoretical approaches. It is important, however, that the results can be compared against the performance of physical systems. Accordingly, a further task of the SINARI project is the development of a physical platform to capture and/or emulate the interactions associated with the interdependent electrical distribution network and ICT infrastructures.

In terms of its overall structure, the existing interactive systems of the electrical distribution network and its supporting ICT based control systems can be broken down into four main sub blocks. These include:

- the physical electrical distribution network;
- the points of localised control & automation, which are placed at key nodes throughout the network;
- the supporting telecommunication systems which permits the points of local automation and control to communicate at a distance;
- the points of centralised intelligence making up the Supervisory Control and Data Acquisition (SCADA) and/or Distribution Management System (DMS).

This functional architecture is summarised in Figure 3.

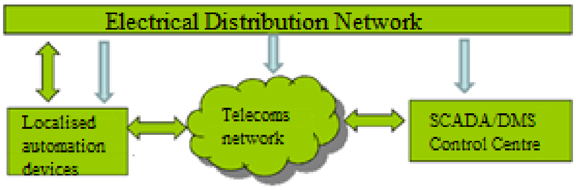

Figure 3 Global functional architecture of electrical distribution network and its supporting ICT

The demonstration platform being developed will be structured in an analogous fashion. The platform is being constructed with four main functional sub-blocks including:

- an emulator of a part for a fragment of an electrical distribution network,
- a number of physical control and automation devices, configured to reproduce their « in-field » performance ;
- a software emulation of the telecommunication system permitting communication between the local points of automation and the control centre ;
- a point of centralised control with functions analogous to those of a modern SCADA / DMS systems;

At the time of writing, integration tests were being completed for the demonstration platform. Final results will be reported once they are available.

2 FMEA – Failure Modes and Effects Analysis
3 HAZOP – HAZard and OPerability Study

Test bank

As a complement to the demonstration platform, a test bank is also being constructed. This system will ensure the initialization of the sub-systems of the platform and will control the parameters used in the different test scenarios.

The tests themselves will focus on both the behaviour of the ICT elements (e.g. CPU charges, memory use, etc) and the impact of ICT performance on the behaviour of the associated synthetic electrical distribution network. Consequences could include delays or failures in the executions of commands and eventual impacts on the number of customers off supply and/or the energy not served.

COUNTERMEASURES & RISK LIMITATION

The final aspect of the project is the development of various approaches for reducing the risk to which an electrical distribution network is exposed due to its use of ICT and the examination of their effectiveness. While an important aspects of the project SINARI, at the time of writing, this task is least advanced within the project. Nonetheless, two main approaches are being explored.

In the first case, the potential value resulting from the use of methods for software verification is being examined. Complementing this, techniques for boosting the resilience of the telecommunication systems used between the electrical distribution network sub-stations and the control centres are being investigated. Focus is being placed on this second approach given that its potential effectiveness can be examined using of the demonstration platform.

CONCLUSIONS

This paper has presented an overview of the project SINARI. Clearly the project has already made significant progress in the modelling and analysis of the vulnerability of interdependent infrastructures, with a particular focus on the use of the ICT to support the operation of the electrical distribution network. The finalisation of the demonstration platform and its eventual application will permit an appraisal of the theoretical results. It will also permit a more robust comparison of the value of the certain techniques for augmenting the overall resilience of the coupled electrical distribution networks and its supporting ICT systems.

Finally, it is important to highlight once again that the project has focused essentially on the current use of the ICT in the existing electrical distribution network rather than an anticipated future distribution network with more pervasive ICT. Even so, it is clear that the cross-domain analysis required to better understand the behaviour of even the existing electrical distribution network is a complex process. The SINARI project has already played an important role in developing these cross-domain competences, which will become increasingly valuable given the expected evolution of the electrical distribution network.

REFERENCES

[1] G. Ericsson, Å. Torkilseng, G. Dondossola, M. Tritschler and L. Piètre-Cambacédès, "Information security for Electric Power Utilities – results of Cigré WG D2.22," *Proceedings of the 43rd CIGRE Session*, Paris, France, August 2010

[2] J.-T. Zerbst, L. Pietre-Cambacedes, G. Dondossola, J. McDonald, M. Ekstedt, "Cyber attack modeling and security graded approach: key elements when designing security architecture for Electric Power Utilities (EPUs)," *44th CIGRE Session, Paris*, France, August 2012

[3] A. Merdassi, R. Caire, et al "Etat de l'art sur les méthodes de modélisation pour les infrastructures critiques interdépendantes", *Proc. Workshop Interdisciplinaire sur la Sécurité Globale (WISG),* Troyes, France, January 2011

[4] Gary Stoneburner, Alice Goguen, and Alexis Feringa. Special Publication 800-30: Risk Management Guide for Information Technology Systems. Recommendations of the National Institute of Standards and Technology (NIST), July 2002. Available at: http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf

[5] Exida, www.exida.com. IEC 61508 Overview Report, version 2.0: A Summary of the IEC 61508 Standard for Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems. White paper, Exida, January 2, 2006

[6] EBIOS (Expression des Besoins et Identification des Objectifs de Sécurité) : Méthode de gestion des risques. Version du 15 janvier 2010 : http://www.ssi.gouv.fr/site_article45.html

[7] MEHARI 2010. Guide de la démarche d'analyse et de traitement des risques. Janvier 2010. CLUSIF : http://www.clusif.asso.fr/fr/production/ouvrages/pdf/MEHARI-2010-Guide-demarche.pdf

[8] MEHARI 2010. Présentation générale. Janvier 2010. CLUSIF : http://www.clusif.asso.fr/fr/production/ouvrages/pdf/MEHARI-2010-Introduction.pdf

[9] Z. Yazar. A qualitative risk analysis and management tool – CRAMM. SANS Institute, 2002.

[10] 2010 CERT Research Report, CERT Information Services, and SEI Communication Design, 2011, http://www.cert.org/research/2010research-report.pdf