Demonstrating Cyber-attacks *impact* on Cyber-Physical simulated environment

Yannis Soupionis
Joint Research Center
European Commission
Institute for the Protection and Security of the Citizen
Via E. Fermi, 2749, 21027 Ispra (VA), Italy
yannis.soupionis@jrc.ec.europa.eu

Thierry Benoist
Joint Research Center
European Commission
Institute for the Protection and Security of the Citizen
Via E. Fermi, 2749, 21027 Ispra (VA), Italy
thierry.benoist@jrc.ec.europa.eu

ABSTRACT

Critical Infrastructures (CIs), such as a smart grid, relay extensively on Information and Communications Technology (ICT) nowadays. In this demonstration, we exhibit a real-time simulation of a smart grid infrastructure and the impact of specific cyber-attacks on it.

1. INTRODUCTION

The explosive growth of the Internet has introduced advanced service which have a great impact on the way we do business. For example, Critical Infrastructure, and especially power grid systems are just one of the many services that rely on computers and the Internet for their operations, such as power balance controlling.

2. SIMULATION ENVIRONMENT

In this demonstration we present a graphical method to illustrate the proper operation of a smart grid network and the impact of a cyber attack on it. The approach leverages two software tools developed within the Joint Research Centre: the Assessment platform for Multiple Interdependent Critical Infrastructures (AMICI)[1] and the EXercise event Injection TOolkit (EXITO)[2]. Specifically, we integrated AMICI software into EXITO in order to enable a graphical user interface for simulation-driven demonstrations and human-actor training. The modular architecture of the framework is given in Figure 1. It includes 3 main units: a) an IEEE bus power grid simulation, which provides the physical process, b) the Remote PLCs, the targets of our attacks, and c) the SCADA system, which controls the power balance. Our demonstration showcases the effectiveness of attacks on terms of voltage instability to power grid and possible cascading effects to other infrastructures,as railway transport and power market.

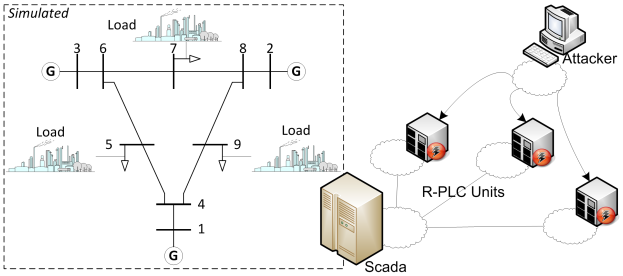

Figure 1: A topology of the simulated environment.

3. CONCLUSIONS

Our demonstrations depict the consequences of ICT disruptions on a simulated power grid. We considered a set of cyber attacks (DDoS and integrity) that are causing a severe telecommunications service degradation and propagates to the operation of other CIs.

4. REFERENCES

[1] B. Genge, C. Siaterlis, M. Hohenadel: AMICI: An Assessment Platform for Multi-Domain Security Experimentation on Critical Infrastructures. 7th International Conference on Critical Information Infrastructures Security, Norway, Lecture Notes in Computer Science 7722, pp. 228-239, 2012.

[2] A. Perez Garcia, C. Siaterlis, and T. Benoist, Technical guidelines for preparing and executing cyber-exercices using EXITO, the EXercise event

Injection TOolkit, JRC Scientific and Technical Report, JRC73562, 2012.