CERCES: Center for Resilient Critical Infrastructures

Mads Dam György Dán Henrik Sandberg Ragnar Thobaben
ACCESS Linnaeus Centre
KTH Royal Institute of Technology, Stockholm, Sweden
Email: {mfd,gyuri,hsan,ragnart}@kth.se

***Abstract*—The newly started CERCES project will develop algorithms, protocols and tools for improving the resilience of critical industrial information and control systems against cyber attacks. This extended abstract outlines the focus areas and the objectives of the project.**

I. Introduction

The MSB (Swedish Civil Contingencies Agency) funded Center for Resilient Critical Infrastructures (CERCES) project aims to improve the resilience of industrial information and control systems used in critical infrastructures against cyber attacks. The project team consists of four research groups at the School of Electrical Engineering and at the School of Computer Science and Communication at KTH, all belonging to the ACCESS Linnaeus Centre. The project started in September 2015 and runs for 5 years.

II. Project Objectives

The objective of CERCES is to develop algorithms, protocols and tools for the prevention, detection and mitigation of cyber attacks on industrial control system components and infrastructures, with an emphasis on Supervisory Control and Data Acquisition (SCADA) systems. The project work is structured in four areas central to critical infrastructure security, with the following aims.

Embedded software platforms: Explore how virtualization-based techniques can be used to meet the demands of current and future SCADA/critical infrastructure platforms, regarding security, trustworthiness, and dependability [1]. The secondary aim, although equally important for industry acceptance, is to meet requirements concerning functionality, real time performance, and cost, and to transfer outputs of the project in terms of know-how, designs, requirements, and code to industry and society.

Wireless communication: Demonstrate that physical-layer security techniques are a powerful means to complement conventional security features of wireless SCADA system infrastructures in order to improve the resilience against attacks in the wireless domain (e.g., eavesdropping, jamming, impersonation), to reduce the security overhead resulting from heavy-weight encryption, and to improve the overall security performance [2]. Focus will be on three aspects of physical-layer security: physical-layer authentication, wireless secret key generation and distribution, and jamming resilient wireless infrastructures.

Communication and computation infrastructures: Develop secure and resilient algorithms and protocols for SCADA communication and computation in shared environments. The algorithms and protocols will leverage knowledge of the physical processes monitored and controlled, and the computations to be executed in order to achieve the best trade-off between performance, cost and security [3]. Focus will be on secure communication protocols for emerging application scenarios, resilience to denial of service attacks, and secure computation on semi-trusted computing platforms.

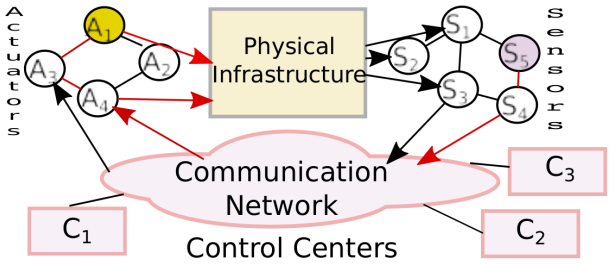

Fig. 1. Sensing to actuation in industrial information and control systems.

Control algorithms: Develop control and monitoring algorithms to ensure resilient operation of critical infrastructures, such as smart grids and traffic systems. We will develop modeling tools that are able to capture the essential behavior of both the cyber and physical components [4]. Based on these, we will be able to perform a vulnerability and impact analysis that serves to identify critical areas in the infrastructure. We can then design application-layer intrusion detection systems that can be incorporated in novel resilient control architectures that are able to encapsulate and attenuate malicious actions.

CERCES will develop a testbed that will consist of wireless sensors, embedded computing devices and a virtualized control environment, and will be used for the experimental validation of the algorithms and solutions developed and for demonstration of the results to industrial partners. CERCES will collaborate with NCS3 at FOI, focusing on education and training, to extend the capabilities of the NCS3 CRATE platform, for interconnecting testbed facilities, and for the promotion of research.

References

[1] M. Dam, R. Guanciale, N. Khakpour, H. Nemati, and O. Schwarz, "Formal verification of information flow security for a simple ARM-based separation kernel," in *ACM Conference on Computer and Communications Security (CCS)*, Oct. 2013.

[2] V. Rathi, M. Andersson, R. Thobaben, J. Kliewer, and M. Skoglund, "Performance analysis and design of two edge type LDPC codes for the BEC wiretap channel," *IEEE Transactions on Information Theory*, vol. 59, no. 2, 2013.

[3] O. Vukovic and G. Dán, "Security of fully distributed power system state estimation: Detection and mitigation of data integrity attacks," *IEEE Journal on Selected Areas in Communications (JSAC)*, vol. 32, no. 7, Jul. 2014.

[4] K. C. Sou, H. Sandberg, and K. H. Johansson, "Data attack isolation in power networks using secure voltage magnitude measurements," *IEEE Transactions on Smart Grid*, vol. 5, no. 1, 2014.