Protection via Cyber Security Event Analysis Framework Using Full-Scope Plant Simulator Capabilities

P. Tsvetkov
Department of Nuclear Engineering, Texas A&M University, MS 3133 TAMU
College Station, TX, 77843-3133, E-mail: tsvetkov@tamu.edu

A. Cardenas
University of Texas at Dallas

M. Manic
Virginia Commonwealth University

J. Wilhelm
GSE Performance Solutions, Inc.

INTRODUCTION

Increasing numbers of cyber security events of various kinds and further expansion of smart technologies in industrial domains, globally, are among the contemporary realities creating the must to further fortify nuclear energy facilities, from nuclear power to nuclear fuel cycle plants. Various solutions and options are being developed.[1] The full scope plant simulators offer realistic near-operator-like control room experiences for operator training purposes. They can be found at all nuclear power plants. Taking advantage of the realistic representation of the control room functions within the full scope simulator framework, the present effort is exploring capabilities, advantages and limitations of using the full scope simulators in the plant protection programs as cyber security event analysis frameworks. This is an opportunity to develop a prototypic intelligent I&C communications analysis system that would be capable of enabling nuclear power plants with current and emerging advanced reactors to recognize potential cybersecurity vulnerabilities and threats, offer threat elimination and consequence mitigation pathways, and optimize resources needed for threat management efforts as an ad-on capability within already existing full scope simulators without disrupting the plant facilities. The cyber security analytics is envisioned as an add-on software package within a digital framework that has capabilities to assess communications and provide cyber resistance via self-awareness. The resulting notification and data management are assumed to yield adaptability to evolving cyber threats. There are considerations for potential insider threats originating from within a power plant as well as for potential disruptions triggered by cyber security attacks on energy grid and power plant interfaces with energy grid including smart grid vulnerabilities. Improved self-awareness and intelligent performance characterization of a power plant state and its communication interfaces with energy grid is becoming increasingly important with the growing integration of analog and digital I&C communications.

THE GSE FULL SCOPE PLANT SIMULATOR

The full-scope simulator (GSE full scope GPWR plant simulator) is utilized in the effort as a development environment and a mock-up implementation facility representing an operating nuclear power plant to develop the proposed communications analysis system and evaluate its performance in real-life operational scenarios. GSE Performance Solutions is the supplier of power plant control room simulations and training solutions and is the developer of the GPWR full scope simulator used in this effort. GSE has designed and manufactured control room simulators for Westinghouse PWR, GE BWR, Combustion Engineering, CANDU, VVER and B&W nuclear plants, and has built well in excess of 250 simulators for fossil fuel plants around the world.

The simulator offers a realistic near-operator-like control room experience of a typical LWR nuclear power plant with PWRs. The existing simulator control room configuration is shown in Fig. 1. The specific simulator configuration consists of working operator stations and VPanels emulating control room systems via touch-sensitive monitors. Each VPanel consists of three vertically-mounted 60 in. touch-sensitive monitors.

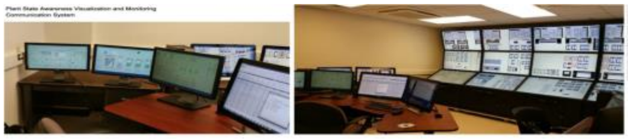
Plant State Awareness Visualization and Monitoring Communication System

Fig. 1. The GSE full-scope GPWR plant simulator at the Nuclear Engineering Simulator Laboratory, Department of Nuclear Engineering, Texas A&M University.

The simulator software is written in JAVA and C++ and has full development capabilities needed for the proposed project including adding additional instrumentation, retrofitting existing sensors, making modifications to plant responses and dynamics to assess cybersecurity events and system and personnel responses and their efficiency, evaluations of plant-energy grid interfaces and their communications.

ANALYSIS FRAMEWORK

The objective is two-fold – (1) parametrize and characterize cyber threats accounting for both inside communications and energy grid initiated attacks and (2) develop an Intelligent Digital I&C Communications Analysis System with self-awareness capability via AI (artificial intelligence) to maximize plant cyber-resistance characteristics taking advantage of the existing full scope simulator infrastructure. The Prototypic Intelligent Digital I&C Communications Analysis System would provide cyber security event analytics and support risk-based prioritization, performance-driven threat containment and cybersecurity team management and education. It is understood and recognized that the existing full scope simulator infrastructure will need to be enhanced with communication architectures and hardware to provide capabilities to emulate real-life plant communication systems within the plant and plant interfaces with the energy grid.

As a system "brain" analysis and interpretation core, an artificial neural network (ANN) approach can be implemented because it is inherently suitable as an architecture for capturing intrinsic interrelationships of highly nonlinear plant communications and Big Data processing driven by large sensor arrays where sensors vary in their physical location as well as in sensing frequency and signal nature.[2] ANN approaches represent a powerful vehicle for processing such large sensor arrays due to inherent feature of ANNs – additional input does not require modification of ANN architecture. It merely requires addition of such input to an existing ANN architecture, i.e. the existing working architecture does not require additional changes. This feature is coming from a definition of an artificial neuron as a weighted sum threshold element.

CONCEPT IMPLEMENTATION AND IMPACT

Improved self-awareness and intelligent performance characterization of a power plant state and its communication interfaces with energy grid is becoming increasingly important with the growing integration of analog and digital I&C communications evolving into smart grid architectures at different levels. The focus on the existing full scope plant simulator capabilities and enhancing them to support cyber security protection measures is a cost-effective approach integrating inherent internal real-time measurements of cyber as well as physical process operations at a plant (as represented in the simulator) in order to build indicators of attacks, preventive metrics and response functions. Industrial control protocol parsers enable deep-packet inspections of the communications between industrial devices focusing on energy grid interfaces in particular as well as data streams within a plant. The deep-packet inspection will help creating a redundant and reliable way to observe the physics of the process under control in order to identify anomalous and potentially hazardous operations.

In addition to security indicators from communication streams and physical observations, the concept will leverage models of traditional cyber-indicators of attacks built on typical network operations and device-to-device communications. Similar to how traditional IT networks are monitored and protected by Security Operations Centers (SOCs) which aggregate a variety of indicators of attacks in dashboards to help security analysts interpret suspicious IT event, the final objective is to be able to integrate different sets of indicators of attacks into a prototype for an Industrial Security Operations Center (ISOC).

This ISOC will integrate suspicious activity from cyber- and physical-anomalies with the goal of presenting operation engineers with security training, information about the state of the plant, and about the cybersecurity of the operational network. When a control center detects a safety problem, for example such as a high pressure in a certain tank or a piping system, steam train, etc., or overheating conditions, there is currently no way to identify in real time if this anomaly originated because of a malicious cyber-intrusion or from a random natural fault or accident in the system. It is also not a trivial task to distinguish the real occurrences from malicious event emulations introduced to disrupt operations without triggering actual physical progressions.

Operators generally tend to assume that these anomalies are due to natural events or accidents.[6] The growing evidence of cyber vulnerabilities and attacks to control systems shows that there is a need to evolve current tools so that operators of physical systems can make informed interpretations of the events unfolding in front of them. The use of the on-site full-scope plant simulators allows for seamless expansions of analytical assistance capabilities taking advantage of various predictive tools, for example, following AI recommendations and making decisions on how to respond to the alerts.

Current practices use physical measurements to show system operators the state of the physical process (power grid, LWR, or SMR, etc.) in traditional Control Centers (CCs) and cyber-security information is collected and displayed to security analysts in Security Operations Centers (SOCs).[5] Today these two types of data are analyzed separately by different people. Operator consoles show the state of the system to operators, and also provide alerts and warnings if there are any safety concerns or faults in the system. Computer networks are part of these operator consoles but their network status has traditionally not been part of the information operators receive. Computer Security Response Teams (CSIRTs) receive and analyze information about the state of networks they are responsible in SOCs.[4] Security Information and Event Management (SIEM) systems usually collect log, connection flows, and intrusion alerts in a unified system allowing security analysts to correlate alarms and improve their situational awareness of the state of security for their system.[5]

Thus, operators in CCs cannot see potential cyber threats and security analysts in SOCs are deprived of information that can help them identify early indicators of cyber-attacks targeting the nuclear power systems. The goal is to design the Industrial Security Operation Center (ISOC) where HMIs and operator consoles detect events and process them to correlate information against cyber-attack indicators as well as physical alerts and anomalies.[3] Cyber indicators of compromise combined with the sensor data from physical observations will provide industrial users with information to help them decide whether or not alarms generated by the physical state of the system are due to random failures or if there is any indication of an attack.

CONCLUSIONS

This paper provides an overview of a plant protection system that takes advantage of the existing full-scope plant simulator capabilities and extends them to form a cyber security event analysis framework integrating early warning systems from cyber-security indicators with safety and physical alerts. The resulting analytics platform supports a comprehensive assessment of the plant state in real time. Cyber indicators of compromise combined with the sensor data from physical observations will provide industrial users with information to help them decide whether or not alarms generated by the physical state of the system are due to random failures or if there is any indication of an attack. State-of-the-art control systems should offer intelligent components for timely reporting and understanding of the monitored plant behaviors in order to increase state-awareness of plant's operators and provide robust and early alarm reporting. The improved control system state-awareness is achieved via fusing input data from multiple sources and combining them into robust anomaly indicators. With a massive amount of collected data, ANN will provide a structure with interconnected units of input and output, creating a functional mapping that is able to accurately model underlying interdependencies between inputs and outputs. This results in an architecture that has unique capabilities for dealing with multi-dimensional nonlinear data. Nuclear engineering expertise is required to account for operational behavior, needs, and requirements. Cyber-security expertise is required to identify and address threats. The full-scope simulator serves as a development environment and a mock-up implementation facility representing an operating nuclear power plant to develop the communications analysis system and evaluate its performance in real-life operational scenarios.

REFERENCES

1. C. BURNS, "Evaluation of Ecological Interface Design for Nuclear Process Control: Situation Awareness Effects", *Human Factors*, **50**, pp. 663 – 679 (2008).
2. M. FAST, T. PALME, "Application of Artificial Neural Networks to the Condition Monitoring and Diagnosis of a Combined Heat and Power Plant", *Energy*, **35**, pp. 1114 – 1120 (2009).
3. G. GU, A. CARDENAS, L. WENKE, "Principled Reasoning and Practical Applications of Alert Fusion in Intrusion Detection Systems", *Proc. 2008 ACM Symp. Information, Comp. and Comm.*, ACM (2008).
4. B. HORNE, "On Computer Security Incident Response Teams", *IEEE Security & Privacy*, **12**, pp. 52 – 60 (2014).
5. M. MANIC, "Data Mining", *The Industrial Electronics Handbook*, 2nd. Ed., Edited by I. Wilamoski, Intelligent Systems, CRC Press, Taylor & Francis (2011).
6. P. TSVETKOV, S. BRAGG-SITTON, J. JOHNS, M. JOHNSON, "3D In-Core Monitoring in Advanced Reactor Environments", *Trans. Amer. Nucl. Soc.*, **106**, pp. 626-627, USA (2012).