Contribution ID: **493** Type: **Paper**

A simulated Steam Turbine Generator subsystem for Research and Training

This paper proposes an approach to simulate a Steam Turbine Generator subsystem focused on a realistic behavior and architecture of the IT-components with the aim of supporting training for cyber-security operators and cyber-security investigators. The scientific contribution of this paper is a description of the Steam Turbine Generator from a computer scientist point of view, the analysis of requirements for such a simulation and the design of an architecture fulfilling these requirements.

Steam turbines form an integral part of any power plant. They perform the task of generating electric power by using the steam pressure generated by the steam generators of the reactor. In general, steam turbines consist of a shaft connected to a number of blades and various valves. The rows of blades are spaced around the shaft so that applied pressure leads to rotation. The valves control the steam flow to the turbine. These components are the actors in this cyber-physical system. As such, the valves are controlled by ICS (Industrial Control Systems) and might be the target of cyber attacks or affected by transmission errors.

Currently, the possible detection of attacks on the ICS controlling valves within Steam Turbine Generators is barely researched, as well as the mitigation of and recovery from potential attacks. This includes the investigation of potential attacks.

Our proposal is to provide a model and simulator with realistic representation of involved hardware, software and communications architecture of a Steam Turbine Generator system. Modeling this Steam Turbine Generator system requires understanding the system from a computer scientist point of view, including computing units, sensors, actuators and the communication between these components. The simulation requires adherence to a realistic behavior of the software components and communication protocols. In addition, this simulation can trigger a pre-defined ranges of unusual behavior, caused by cyber events, operator error or attrition of components.

In contrast to a physical mock-up or a control room simulator, such a simulation aims at being easy to deploy, easy to alter and easy to scale. It focuses on the IT-components and not only on physical processes. Hence, it can serve as a foundation for a.) research into cyber-security measures like techniques for detecting or mitigating attacks, b.) training platform for cyber-security operators with regards to detection and mitigation of cyber-events, c.) training for cyber-security investigators by allowing investigation into the IT-components and d.) for operators in terms of recovery from a cyber-event caused error within a subsystem.

The simulation proposed in this paper is demonstrated using PLCSIM Advanced to create virtualized PLCs. This allows easy deployment for training purposes. The virtualized PLC communicates (physical) process variables using OPC UA with the simulation module, making this approach more scalable. This simulation module handles the underlying physical process and provides the virtualized PLC with realistic input via the PLCSIM Advanced API. The simulation module is programmed in C# and allows for easy alteration or extension of the system setup. In addition, the simulation module is able to inject various cyber events, errors and jitter to the transmitted data. In addition, a local HMI is included to give a system operators view to a potential trainee or investigator. This architecture allows the researcher access to the 'physical reality' of the simulated process as well as the 'PLC reality' (how the physical process performs from the viewpoint of the PLC) as well as the 'Operator reality' (how the physical process performs from the viewpoint of the Operator).

The final submission will include the architecture of the simulator, a definition of the communication flow, a definition of various fault states and attacks available from the simulator and an investigation into potential forensic traces within the network communication and the attached PLCs.

Gender

Not Specified

State

Germany

Authors: ALTSCHAFFEL, Robert (Otto-von-Guericke Universität Magdeburg); HILDEBRANDT, Mario (Otto-von-Guericke-University of Magdeburg); Prof. DITTMANN, Jana (Otto-von-Guericke-University of Magdeburg)

Presenters: ALTSCHAFFEL, Robert (Otto-von-Guericke Universität Magdeburg); HILDEBRANDT, Mario (Otto-von-Guericke-University of Magdeburg)

Track Classification: CC: Information and computer security considerations for nuclear security