A SIMULATED STEAM TURBINE GENERATOR SUBSYSTEM FOR RESEARCH AND TRAINING

R. ALTSCHAFFEL
Otto-von-Guericke University
Magdeburg, Germany
Email: Robert.Altschaffel@iti.cs.uni-madeburg.de

M. HILDEBRANDT
Otto-von-Guericke University
Magdeburg, Germany
Email: Mario.Hildebrandt@iti.cs.uni-madeburg.de

J. DITTMANN
Otto-von-Guericke University
Magdeburg, Germany
Email: Jana.Dittmann@iti.cs.uni-madeburg.de

Abstract

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 a design of an architecture fulfilling these requirements.

1. INTRODUCTION

Training is a major component of improving safety in NPP (Nuclear Power Plant) environments. Hands-on-Training requires access to expensive and rare systems inducing a high cost and low accessibility. To counter these problems, various simulators exist implementing some functions of NPPs in order to facilitate training, like PCTRAN[1]. These simulators focus on the physical processes and the plant operations. They are not geared towards a realistic representation of the control hardware involved during these plant operations. The control hardware consists of sensors (providing information about the physical process), computing units (calculating adjustments to the physical process) and actuators (altering the physical process).

These functions are referred to as I&C systems (Instrumentation & Control systems) and are not the focus of these training tools. Hence, training to react on faults in these I&C systems (e.g. a sensor providing faulty readings) is outside of the scope of these tools. This goes for faults caused by wear and tear as well as to faults caused by malicious attacks.

In order to support cyber incident response training, we propose a simulator of an NPP subsystem implementing a realistic representation of the involved hardware, software and communications architecture. This simulator is easy to deploy and 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-component, d.) for operators in terms of recovery from a cyber-event caused error within a subsystem. and e.) for analysis of single components within a simulated system environment.

[1] http://www.microsimtech.com/pctran/

2. FUNDAMENTALS

This section provides some background required for a better understanding or our work. It starts with some information about simulators and then gives a short overview on the subsystem chosen for our simulator - the Steam Turbine.

2.1. Simulators

Simulators imitate processes. Usually, simulators imitate physical processes in order to enable the influence of various factors (like user input) to these processes. As such, a simulator requires a model of the underlying physical process in order to ascertain the influence of the various factors. As models, simulators are geared towards certain tasks and have system borders - or scopes. For example, a simulation of a steam turbine might include thermodynamics from the steam flow but might not include calculations to ascertain the wear and tear of the various internal components during the simulated operation. However, some models - those geared towards evaluating mechanical failures - might include such factors into their scope and therefore their modeling.

In general simulators are simulating the physical processes and the influence actors (the active part of the control system) have on these processes. The process of measuring the physical variables, computing it and then sending a control signal to an actor is beyond the scope of these simulators.

While cyber-attacks might eventually aim at altering the physical process, they attack the I&C systems. Hence, in order to take cyber-attacks into account, a simulator including the behavior of I&C components is required. These consists of sensors, computing units and actors. While sensors and actors are relatively simple components, this does not hold true for computing units. Programmable Logic Controllers (PLCs) are complex embedded systems. However, different approaches exist to simulate these complex systems:

- **SoftPLC:** Implementations of PLCs running completely in software, like OpenPLC[2]. These SoftPLCs can read data from sensors and write command to actors just like any normal PLC but do behave internally like real PLCs. Hence, the communication between the PLC and the sensors, actors and potential other PCLs will be realistic while internal processes are not realistic.
- **Simulated PLC:** In this case, the run time environment of a PLC is emulated. A purpose-built implementation a real PLCs specification is implemented. This is mostly used to test specific PLC programs. Examples include PLC-SIM, which is part of TIA Portal[3] used for configuring Siemens PLCs . While a simulated PLC behaves internally like a PLC, it does not use the same internal software (firmware) like the PLC which specification it implements. Hence, it might have other software bugs. In each case, the communication between the PLC and the sensors, actors and potential other PCLS will be realistic.
- **PLC Firmware in Emulator:** In this case, the same firmware that runs in a PLC runs in an emulator on a desktop computer. Examples for this include PLC-SIM-Advanced[4]. Since the same implementation runs on either emulator or PLC, the same bugs are present. Here, PLC behavior as well as communication with sensors, actors and other PLCs is realistic. However, due to the simulation, some aspects of a physical PLC might be still missing.

---

[2] https://www.openplcproject.com/

[3] https://new.siemens.com/global/en/products/automation/industry-software/automation-software/tia-portal.html

[4] https://support.industry.siemens.com/cs/document/109754093/trial-download-simatic-s7-plcsim-advanced-v2-0?dti=0&lc=en-WW

2.2. Steam turbines

Steam turbines form an important part of any power plant. They perform the task of generating electric power by using the steam flow generated by a steam generator [1]. Steam from the secondary side of the steam generator enters the turbine generator and exits to the moisture separator-reheaters [2].

In general, steam turbines consist of a shaft connected to a number of blades [3]. These blades form blade rows and are formed so that the connected shaft revolves once steam pressure is pushing against these blade rows. The generator uses this rotation to create electrical power.

In order to improve flow characteristics inside the turbine a number of static diffusers and bends might be connected upstream. Turbines need a constant stream of steam with specific a temperature and pressure range. To ensure these conditions are met and maintained, steam turbine governing (STG) is used. Sensors attached to the STG deliver information about the state of the system while the actuators (in this case the valves) try to alter this state in order to sustain the specific working conditions. Errors or incidents in this governing can influence the specific parameters and led to reduced efficiency, breakdown or direct damage to the involved components. In addition, the Steam Turbine contains various sensors and actuators to ensure the desired temperature and pressure ranges.

Since various variants of steam turbine assemblies exist, it is necessary to create a generalized model as a foundation for the simulation discussed in this work. This model should contain the components each steam turbine governing assembly shares. The model assumes one turbine, feed by two steam generators. The steam generators feeds into a header for load balancing. Hence, the steam received by the two turbines should have the same properties.

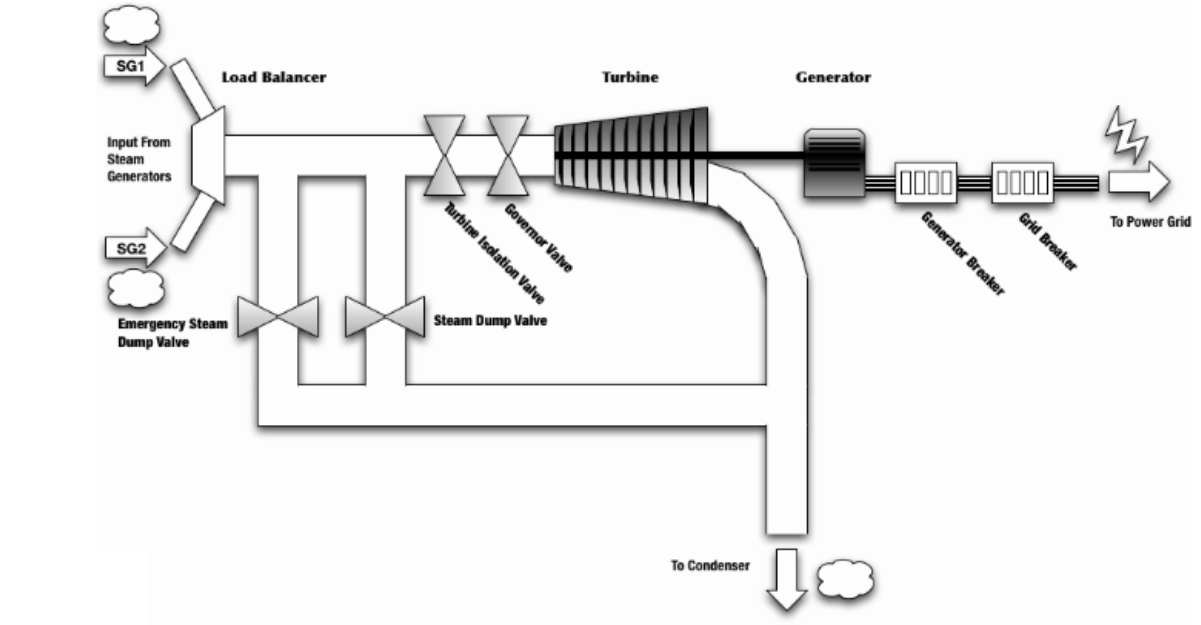

Fig. 1. Steam Turbine Model

As seen in Fig. 1., the steam passes the Emergency Steam Dump Valve, the Steam Dump Valve (also referred to as Main Steam Relief Valve), the Turbine Isolation Valve (also referred to as Main Steam Isolation Valve) and the Governor Valve. The Turbine Isolation Valve is used to isolate the steam source from the generator [4]. If the Turbine Isolation Valve is closed, the Emergency Steam Dump Valve opens in addition to the Steam Dump Valve to redirect the steam flow directly to the condenser. The Steam Dump Valve [5] ensures that only a given maximum pressure is able to pass through the circuit. If the pressure exceeds this maximum, the valve opens and releases the excess pressure.

After the steam passed the Turbine Isolation Valve, the Governor Valve ensures that the steam meets the demanded properties. The Steam is then used to rotate the shaft inside the generator. Steam passing the Turbine, the Emergency Steam Dump Valve and the Main Steam Dump Valve is then directed on to the condenser, while the rotation is used for energy generation.

The control narrative is implemented by the I&C system. Sensors gather information about temperature and pressure while computing units compute the control signals on which the actors - valves in this case - then act. This narrative can consist of four distinct cases:

- **Normal Operation:** During normal operation, the Turbine Isolation Valve is open and the Emergency Steam Dump Valve and the Steam Dump Valve are closed, leading the steam to pass unaltered to the turbine, generating energy in the generator. The turbine will direct the steam to the condenser.
- **Start-up Procedure:** If the turbine is not spinning at all, the control system will speed it slowly up to the setpoint by feeding a small amount of steam into the turbine. The Emergency Steam Dump is closed, The Turbine Isolation Valve is open.
- **Excess Steam:** If the steam pressure exceeds a given limit, the Steam Dump Valve will (partly) open. The excess steam will be directed towards the condenser. The reduced steam will pass on to the turbine, generating electrical energy in the generator. The steam that reached the turbine will be directed to the condenser.
- **Trip:** If a turbine trip is triggered, Turbine Isolation Valve is closed and the Emergency Steam Dump Valve and the Steam Dump Valve are opened. All steam will pass directly to the condenser. The turbine will not be powered by steam and hence no energy will be produced in the generator. In this case, a notification to the operator is necessary. In addition, a direct signal of this occurrence to the reactor, the condenser and the electric power system is necessary. In addition, the breaker will be opened in order to disconnect the power output from the electrical system.

3. CONCEPT FOR AN I&C SIMULATOR

This section presents our concept for an I&C simulator. First, requirements for making such a simulator in a way to be useful for research and training are discussed, before the resulting design is discussed.

3.1. Requirements to an I&C simulator

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, the simulation needs to include some unusual behavior which might be caused by cyber events, operator error or attrition of components. For example, the possibility to have a sensor relay wrong information might represents a faulty sensor or a manipulation of the sensor. Simulating more complex cyber-attack scenarios like an injection attack where an attacker injects messages into the communication require interfaces within the simulator.

In contrast to a physical mock-up or a control room simulator, such a simulator 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 training and research in matters of cyber security.

3.2. Design of an I&C simulator of a steam turbine

The simulation proposed in this paper is demonstrated using PLCSIM Advanced to create virtualized PLCs as depicted in Fig. 2. 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 PLCs with realistic input via the PLCSIM Advanced API.

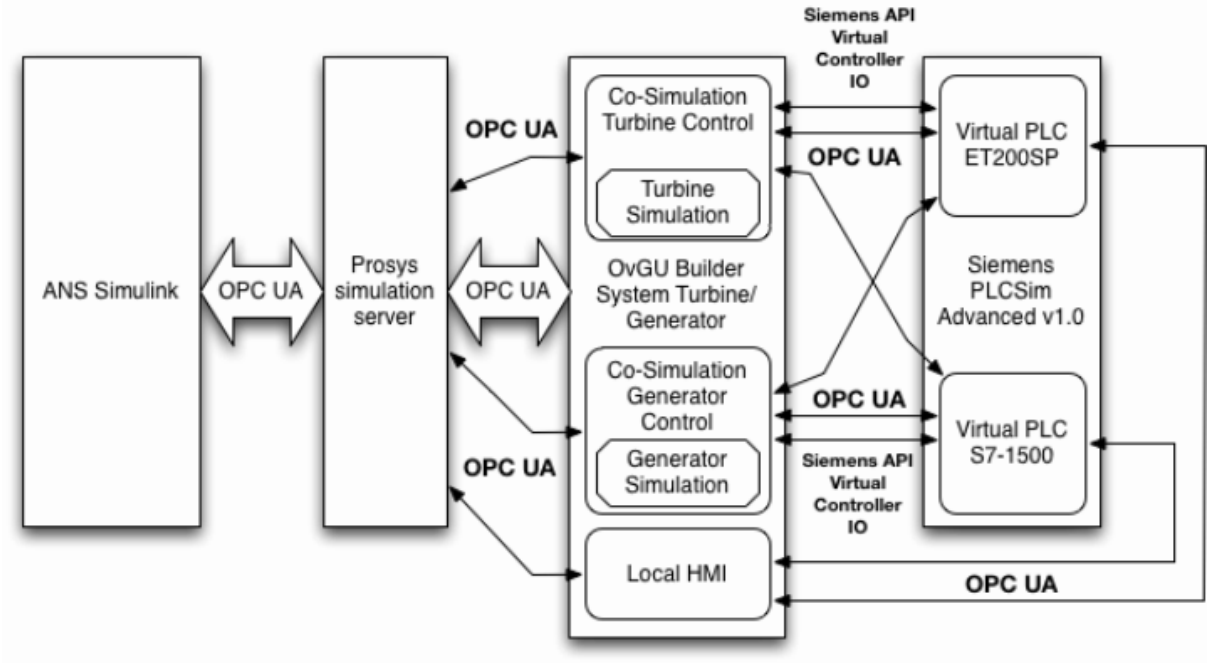

Fig. 2. Architecture of the Simulator

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. Additionally, a local HMI is included to give a system operator's view to a potential trainee or investigator. This architecture allows the researcher access to the 'physical reality' of the simulated process (hence, rather 'model reality') 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). Finally, the simulation could be connected to a simulation of an entire nuclear power plant via OPC UA. In our example we use the ASHERAH Nuclear Simulator [6] for that purpose.

3.2.1. Control Logic and Simulation of the Turbine Governing System

The simulation for the turbine governing system simulates an abstract model of the turbine with its rotational energy. The input for the simulation is the steam generated by the two simulated steam generators. Values for the temperatures, pressures and mass-flow are being read from the OPC UA server, in this case the Prosys Simulation Server[5], as input variables. Furthermore, the grid frequency is read from the OPC UA server as well. This particular value is used as a set point for the rotational speed of the turbine. As a simplification, the rotor is modeled as a cylinder with a mean radius of 2.5 meters and a mass of 100 metric tons inside of the simulation as well as in the PLCs programming. The sensors for temperature, pressure and mass-flow are directly connected to the virtual PLCs analogue inputs in a three-fold redundancy. The PLC calculates the reading from the sensors and issues a signal if a set of sensors are reporting mismatching readings.

During the start-up phase the turbine governing valve is opened until a pre-defined mass-flow is detected through the turbine causing it slowly to spin up. During this start-up phase the rotational energy of the rotor is slowly increasing. As soon as the target speed has been reached, the Governor Valve will be further opened and the Steam Dump Valve gradually closed. In addition to that, the PLC will calculate the available energy that can be used to generate electricity. The friction of the rotor is modeled as a static loss of energy.

[5] https://www.prosysopc.com/products/opc-ua-simulation-server/

If the grid frequency as the setpoint for the turbine speed drops to zero, the turbine governing system assumes a loss of offsite power. In this case the governing valve is closed to a certain level limiting the available energy to the house-load demand to power the plant.

3.2.2. Control Logic and Simulation of the Generator Control System

The generator control is rather simple. It reads the grid frequency, the turbine speed, the status of the breaker command and the available amount of energy from the OPC UA server. If the breaker command is set and the turbine speed would result in electricity being generated matching the grid frequency, the generator breaker will be closed. Then, the generator will produce electricity with the amount of available energy. As soon as the generated amount of electricity exceeds a threshold setpoint, the grid breaker will be closed as well. The generator control also simulates the grid frequency stabilizing effect of large turbines - if the grid frequency drops, additional energy will be used from the rotational energy of the turbine, increasing the output while slowing down the turbine to match the new grid frequency. In the case of a turbine trip, the generator is used to slow down the turbine while producing electricity for the operation of the plant.

3.2.3. Local HMI

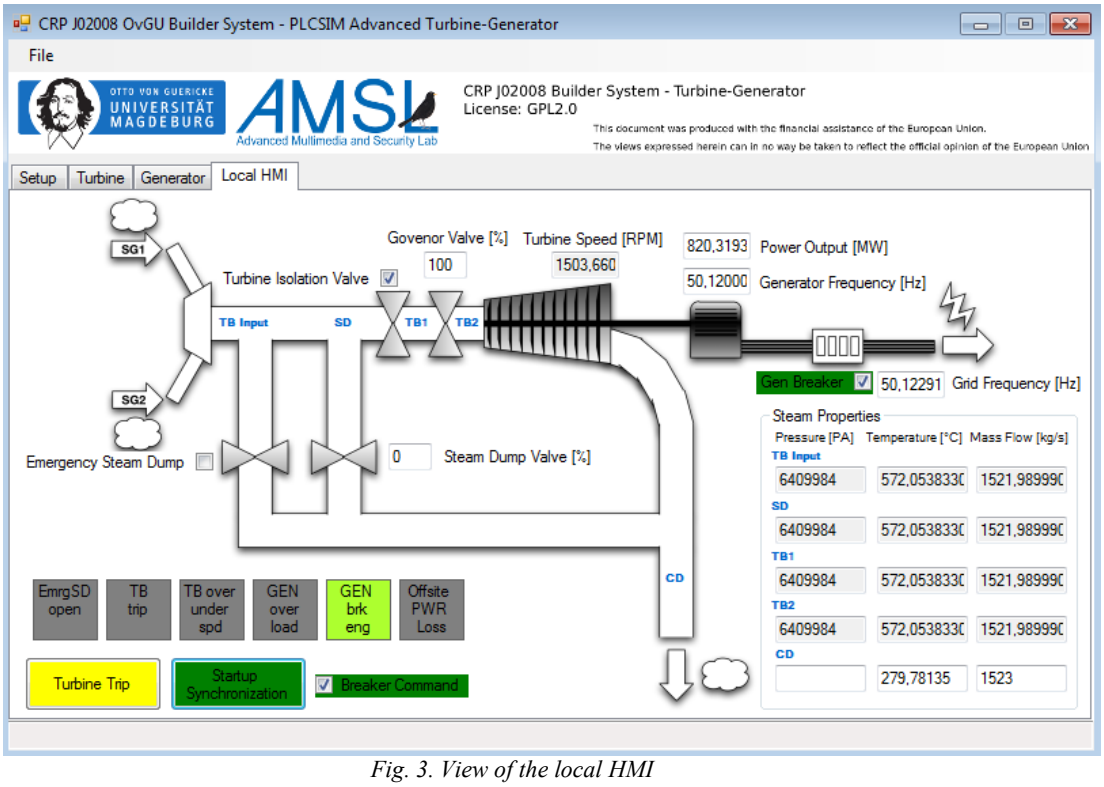

Fig. 3. View of the local HMI

The local HMI for the simulator is depicted in Fig. 3. It contains buttons for controlling the simulation in the lower left corner: the turbine could be tripped; a stopped turbine could be synchronized with the grid and the breaker command could be set. Above those inputs a limited set of annunciations is integrated, informing the operator of:

- an opened Emergency Steam Dump,
- a triggered turbine trip,
- over-/under speed of the turbine,
- overload of the generator (generator power exceeding the design specifications),
- the status of the generator breaker,
- loss of offsite power.

In addition to this, various sensor readings are displaying the current status of the simulation. The displays in the lower right corner show the steam properties at different positions within the turbine generator assembly. If a sensor fault is detected, the specific reading will be highlighted with a yellow background color.

4. USE-CASES

This section discusses the potential use cases in which the simulator can be employed and some advantages we see in using such a simulator.

4.1. Training

As the simulator includes a local HMI which can be used to operate the simulated Steam Turbine, it can be used for training. The normal operation (including a potential start-up procedure) can be used to familiarize trainees with the operation of a Steam Turbine. In addition, the simulators allow for the simulation of failures in various components. For example, a set of sensors readings could be unavailable or faulty. This enables the trainees to train various reaction strategies in order to be prepared in case of an incident.

During examination, the possibility to take a look at 'model reality', 'PLC reality' and 'Operator reality' is highly useful offers tremendous opportunities to better understand the inner workings of a Steam Turbine and its I&C systems.

4.2. Security Evaluation

As the simulator uses realistic communication between the virtualized components, the setup could also be used to analyze attack patterns (as combinations of the five basic attacks: read, interrupt, change, create, steal - see [7]) and potential indicators of compromise (IoC). The specific values in the local HMI are being read from the OPC UA servers running on the PLCs. In addition to that, the readings are exported via the simulator to the Prosys Simulation Server. If an HMI is connected to this server as well, any discrepancies between the two HMIs can be considered as an IoC triggering further investigations.

The communication of the components allows for the inclusion of one more basic attacks in order to evaluate the effect of such an attack. A simple type of attack is a man-in-the-middle attack (a change attack) altering specific readings, e.g. from the Prosys Simulation Server to the simulator. By doing this, the control system could be forced to trigger an unexpected behavior, for example reducing the power output of the generator. The aftermath of such an attack could be used to search for specific traces that are left behind on the components for developing new forensic techniques. Furthermore, specific measures for the incident prevention and detection can be analyzed towards their effectiveness.

Additionally, all this data can be recorded and used for post-incident forensic analysis in order to increase forensic capabilities by providing procedures for potential real incidents.

5. SUMMARY AND OUTLOOK

This work presented an easy to deploy simulator of an NPP subsystem including a realistic representation of the involved hardware, software and communications architecture. This simulator is fully virtualized and hence, cheap and easy to deploy. It can be used for the training of operators and cyber-security experts by triggering various fault states or different attacks on the simulated subsystem.

Further benefits result from the possibilities it offers in terms of research capabilities into the field of NPP cyber-security. The simulator allows for an analysis of the possibility and impacts of potential attacks on NPP I&C systems by creating a realistic representation of the digital technology used within such a control system.

Potential future work would include the simulation of different subsystems to create more complex environments. The inclusion of different types of PLCs and protocols might also increase the potential for training and research.

ACKNOWLEDGEMENTS

This document was produced with the financial assistance of the European Union. The views expressed herein can in no way be taken to reflect the official opinion of the European Union.

REFERENCES

[1] U.S. NRC, https://www.nrc.gov/reactors/pwrs.html, 2015, Last Accessed: 11/27/2019

[2] Westinghouse Electric Corporation, "The Westinghouse pressurized water reactor nuclear power plant", http://www4.ncsu.edu/~doster/NE405/Manuals/PWR_Manual.pdf, 1984, Last Accessed: 11/27/2019

[3] DICK, E., Fundamentals of Turbomachines, Springer, Dordrecht (2015).

[4] http://docs.sempell.com/docs/en/products/nuclear/secondary/MainSteamIsolationValves.pdf, Last Accessed: 11/27/2019

[5] http://docs.sempell.com/docs/en/products/nuclear/secondary/MainSteamSafetyReliefValves.pdf, Last Accessed: 11/27/2019

[6] ALTSCHAFFEL, R. et al., "NPP in a Box" to be presented at ICONS 2020

[7] CLAUSING, E., FISCHER, R., DITTMANN, J., DING, Y., "Your Industrial Facility and Its IP Address: A First Approach for Cyber-Physical Attack Modeling", 35th International Conference, SAFECOMP 2016, Trondheim, Norway, September 21-23, 2016, Proceedings