Simulation Model for Threat and Impact Analysis on Modern Electrical Power Systems

Deeksha Gupta[1], Yongjian Ding[2], Dharini Govindaraj[3], Mathias Lange[2], Martin Szemkus[2], Karl Waedt[4]

Abstract: The increase in interconnected devices in electrical power systems raises the attack surface of a network and therefore the system connected within the network. Cyber-attacks can lead to power cut of an individual system or multiple systems required in the power generation stage and critical in normal operation of the plant. With the purpose to monitor and understand the impacts of cyber-attacks at the component level, system level and plant level, a testbed simulation environment for the Electrical Power Systems in a virtual power plant was modelled. This paper provides comprehensive information about the developed Simulink model for the electrical power system. The Simulink model was created to leverage freedom of customizing and testing of diverse cyber threat scenarios. The simulation model was set to communicate with physical controller to analyse the system level and plant level impacts of cyber-attacks on the physical devices.

Keywords: Cybersecurity; Matlab Simulink Model; Electrical Power System

1 Introduction

Cybersecurity issues in power systems have long been discussed. The simulated Aurora attack on an electrical power generator confirmed that vulnerabilities in protection systems could be exploited in order to cause severe damage to power system components [Ze11]. In order to keep the security of the Industrial Control Systems (ICS) and Electrical Power System (EPS) intact, it requires training of the individuals working on these systems. However, it is dangerous to conduct research and training directly on an operating commercial power plant, as minor disturbances can significantly lead to a negative impact on environment and economy. Therefore, a simulation model is necessary to leverage freedom of customizing and testing of diverse cyber threat scenarios [Gu20a].

The three stages of electric power supply are generation, transmission and distribution. After electrical power is generated at a power plant, it is transmitted over distances

[1] Technical University Dresden, Faculty of Electrical and Computer Engineering, 01069 Dresden, deekshagupta27@gmail.com

[2] Magdeburg-Stendal University of Applied Sciences, Institute of Electrical Engineering, 39114 Magdeburg, yongjian.ding@h2.de, mathias.lange@h2.de, mszemkus@icss.de

[3] Hochschule Darmstadt, Department of Electrical Engineering and Information Technology, 64295 Darmstadt, dharini.govindaraj@stud.h-da.de

[4] Framatome GmbH, 91052 Erlangen, Karl.Waedt@framatome.com

doi:10.18420/inf2020_35

using transmission line and the distribution system connects the transmission system to the consumers. Cybersecurity issues for electrical power systems in transmission or in distribution stages have long been discussed. However, there is very limited information available directing specifically cyber-attacks on EPS in generation stage. Therefore, the main focus of the simulation model was kept on electrical power systems in generation stage and located inside a nuclear power plant (NPP) [Gu20a].

A simulation environment was modelled to understand the physical process of EPS in a virtual nuclear power plant and also to analyse the impacts of cyber-attacks on EPS. Beyond the integration of the interface of the EPS model with the real digital devices, a key benefit for the plant personnel is the exercising and training of “what if” scenarios. These scenarios were simulated in the model and the model computed and showed the impacts at the component level, system level and plant level [Gu20b]. The analysed threat scenarios using simulation model include –data manipulation, availability attack, false data injection, Falsie trip command, etc. Additionally, the simulation model was set to communicate with physical devices (e.g. PLC) to analyse the effects of cyber-attacks on the devices. Open Platform Communications Unified Architecture (OPC UA) communication protocol [IE10] was used to setup the communication between the Simulink model and physical devices.

2 Simulation Model Design

Matlab Simulink tool was utilized to design the EPS simulation platform. The basic design of developed EPS Simulink model of the Electrical Power System was divided into the following 3 parts [Go19]: Power Generation, Grid Feed, and House Load (e.g. cooling system).

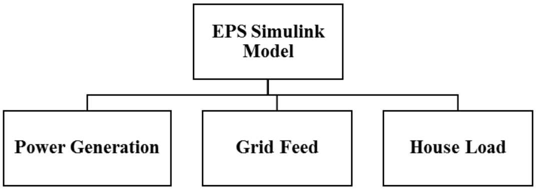

Fig. 1: Proposed EPS Model

3 Block Diagram of Simulink Model

The block diagram of the designed EPS Simulink model is represented in Fig. 1. The model focused mainly on start-up mode and normal operation mode, where the impact of the cyber-intrusion will be highest. Normal operation mode is the stage when the cooling loops require working at the demanding efficiency. Execution of attack in this state would lead the malfunctioning of the cooling system [Go19].

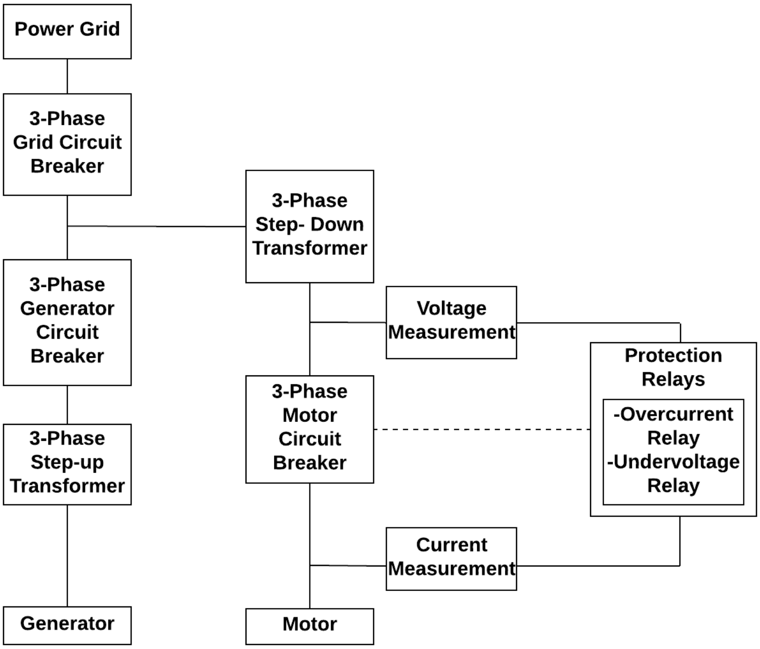
Power Grid
3-Phase Grid Circuit Breaker
3-Phase Step- Down Transformer
3-Phase Generator Circuit Breaker
Voltage Measurement
Protection Relays
-Overcurrent Relay
-Undervoltage Relay
3-Phase Motor Circuit Breaker
3-Phase Step-up Transformer
Current Measurement
Generator
Motor

Fig. 2: Block diagram of EPS Simulink Model [Go19]

4 Implementation of Simulink Blocks

The picture of the Matlab Simulink Model is shown in Fig. 3. The Model is divided into 3 parts—first part includes Plant operations with specific attention on EPS, the second part focuses on control operation, finally, OPC communication module is the third part responsible to set up OPC communication between MATLAB Simulink mode and PLC [Go19]. This section provides the overview of the components in each part.

4.1 Power Generation

Power Generation module comprises components that are directly related to the power generation systems in an NPP. Fig. 4 demonstrates the Power Generation module that includes the following components: (1) Synchronous Generator; (2) Step-up Transformer; and (3) Circuit Breaker.

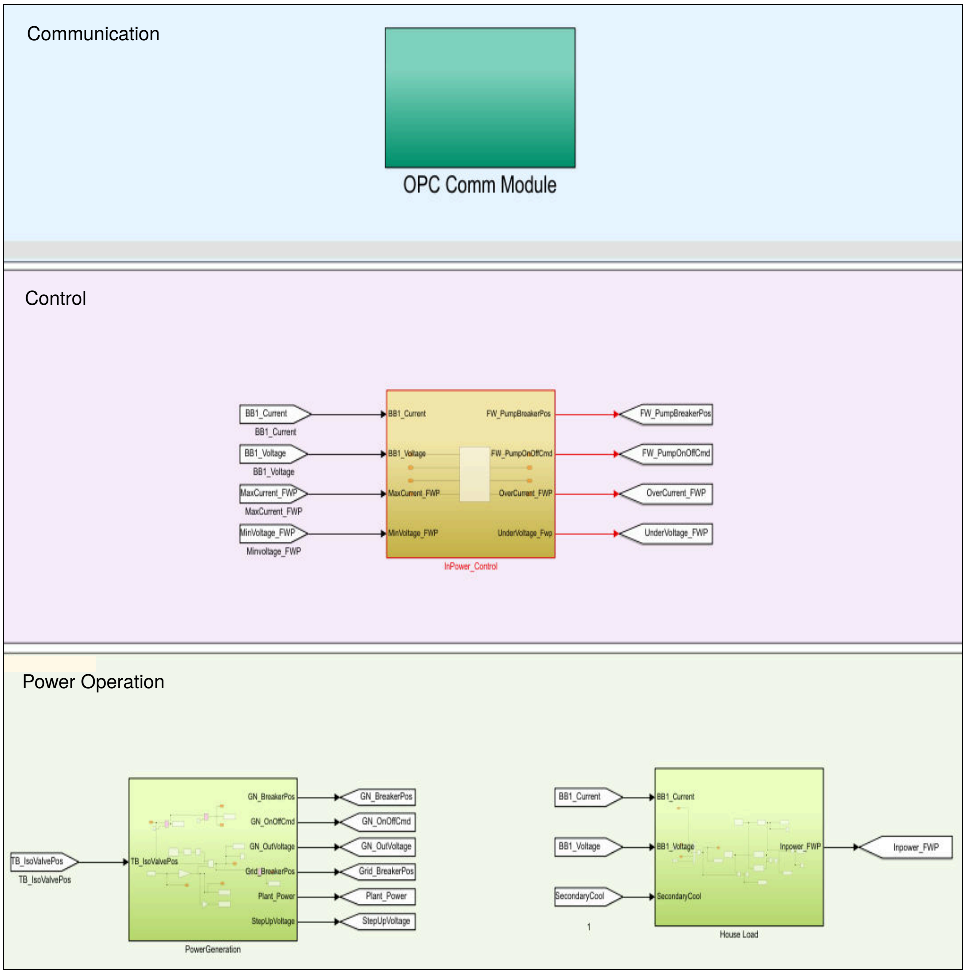

Fig. 3: Overview of MATLAB Simulink Model

4.2 Grid Feed

Fig. 5 shows the Grid Feed module that comprises the components of a simple power grid. This module encloses the following components: (1) Three-phase Source; (2) Transformer; (3) Three Phase; and (4) PI Section Line and Series RLC load.

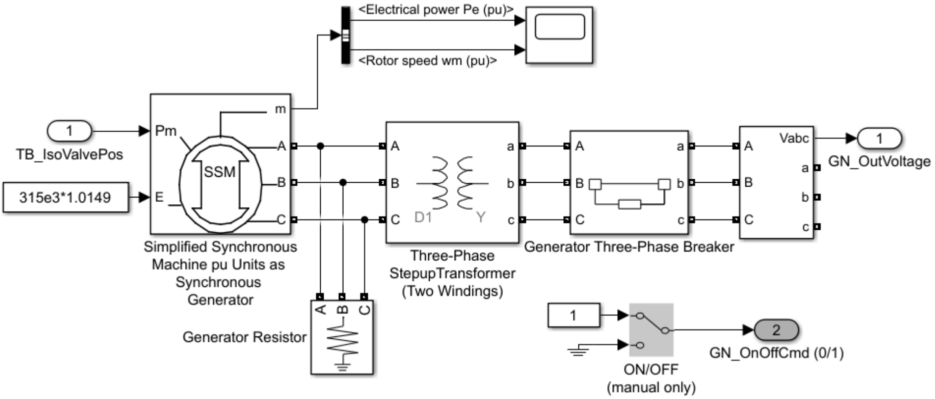
<Electrical power Pe (pu)>
<Rotor speed wm (pu)>
m
1
Pm
TB_IsoValvePos
SSM
A
B
C
315e3*1.0149
E
Simplified Synchronous Machine pu Units as Synchronous Generator
A
B
C
a
b
c
D1
Y
Three-Phase StepupTransformer (Two Windings)
Generator Three-Phase Breaker
Vabc
1
GN_OutVoltage
Generator Resistor
1
2
GN_OnOffCmd (0/1)
ON/OFF (manual only)

Fig. 4: Power Generation

4.3 House Load

Fig. 6 shows the modelled house load module in Simulink model. For the simplicity of the model a Feed Water Pump (FWP) is considered as house load. In a real power plant, house load encompasses multiple electro-mechanical machineries. House load module has the following electrical components: (1) Step-Down Transformer; (2) Circuit Breaker; (3) Asynchronous Motor; (4) Measurement Devices (current measurement and voltage measurement devices); and (5) Protection Devices for undervoltage and overcurrent protections.

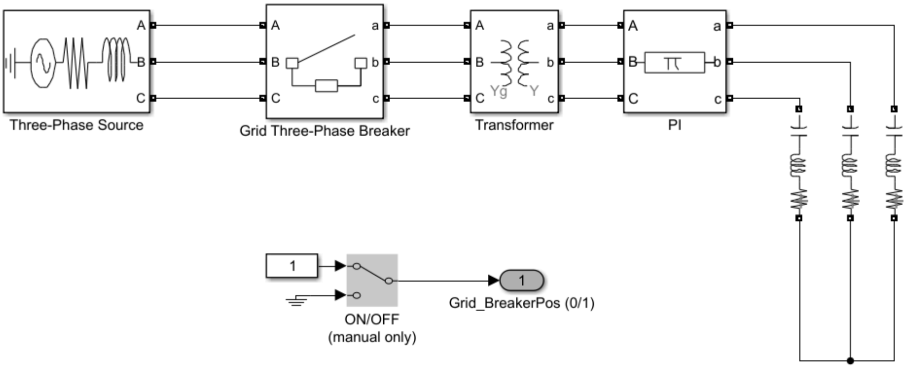

Fig. 5: Grid Feed Module

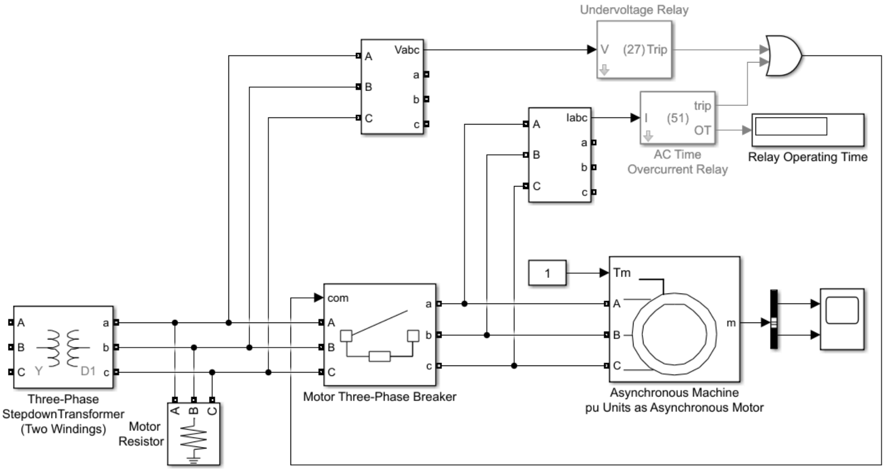
Undervoltage Relay
V (27) Trip
Vabc
A
B
C
a
b
c
Iabc
I (51) trip
OT
AC Time Overcurrent Relay
Relay Operating Time
1
Tm
m
Asynchronous Machine pu Units as Asynchronous Motor
com
Motor Three-Phase Breaker
Three-Phase StepdownTransformer (Two Windings)
Y
D1
Motor Resistor

Fig. 6: House Load

5 OPC UA Communication between Matlab Model and PLC

An OPC UA communication protocol was established between the simulation model and the industrial controller by keeping in mind future scope implementation of communication between different hardware devices from different vendors. Fig. 7 shows details of the OPC Communication module. It can be observed from the figure that Simulink model includes four analog inputs and two digital inputs (total 6 inputs) and six analog outputs and five digital outputs (total 10 outputs). Tab. 1 elaborates the significance of each OPC tag that were used to transfer different parameter values from the Simulink model to the PLC and vice-versa.

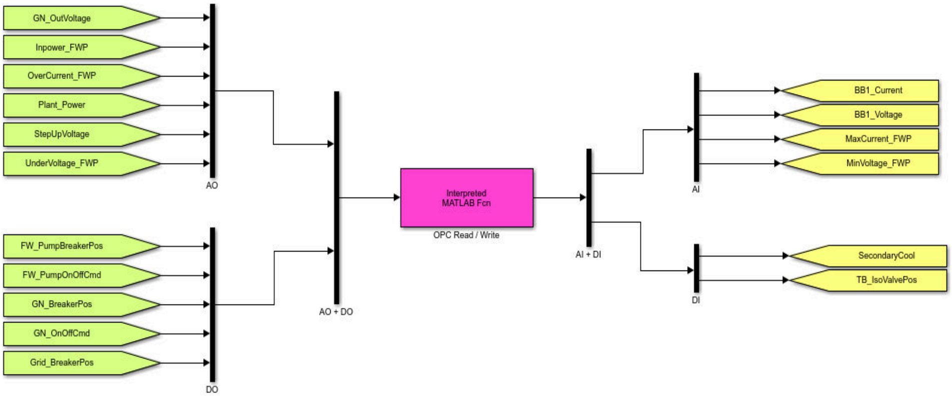

Fig. 7: OPC Tags for Communication

Tab. 1: OPC UA Tags Utilized in Simulink Model

Tag Type	*Tag Name*	*Significance*
Analog Input	BB1_Current	Value of current in Bus Bar 1
	BB1_Voltage	Value of voltage in Bus Bar 1
	MaxCurrent_FWP	Maximum permissible current to FWP
	MinVoltage_FWP	Minimum allowed voltage to FWP
Digital Input	SecondaryCool	State [On/Off (1/0)] of secondary cooling
	TB_IsoValvePos	Position [Open/Close (0/1)] of turbine isolation valve
Analog Output	GN_OutVoltage	Value of generator Voltage
	Inpower_FWP	Value of consumed power by FWP
	OverCurrent_FWP	Overcurrent set-point of FWP
	Plant_Power	Calculated power of a virtual NPP
	StepUpVoltage	Value of voltage of step-up transformer
	UnderVoltage_FWP	Undervoltage set-point of FWP
Digital Output	FW_PumpBreakerPos	Breaker position [Open/Close (0/1)] of FWP
	FW_PumpOnOffCmd	Status [On/Off (1/0)] of FWP
	GN_BreakerPos	Breaker position [Open/Close (0/1)] of generator
	GN_OnOffCmd	Status [On/Off (1/0)] of generator
	Grid_BreakerPos	Breaker position [Open/Close (0/1)] of main grid

6 Attack Implementation and Network Monitoring

The Matlab/ Simulink model, working on a Windows OS computer, was connected with other physical devices for attack implementation as shown in Fig. 8. Various Commercialized devices were used in this hardware-in-the loop (HIL) setup to perform the potential advanced threat scenarios. For our research purposes, an advanced industrial controller was selected. A medium sized (12 inches) PC-based commercial HMI-system was chosen as an Operator Panel. Attacker computer was a Linux based OS, including multiple open source tools for network protocol analysis and execution of cyber-attacks. A windows OS based network monitoring computer was connected to the network switch via a LAN tap to monitor the network traffic. Furthermore, in order to enhance the impact analysis capabilities and set up data transfer via OPC UA communication protocol between Simulink model and the physical device, PLC was programed with control logics and diverse electrical protection functions of a motor protection relay. The main protection functions, considered in this research work cover – thermal overload, overcurrent, undervoltage, and start time supervision protections [Gu20a].

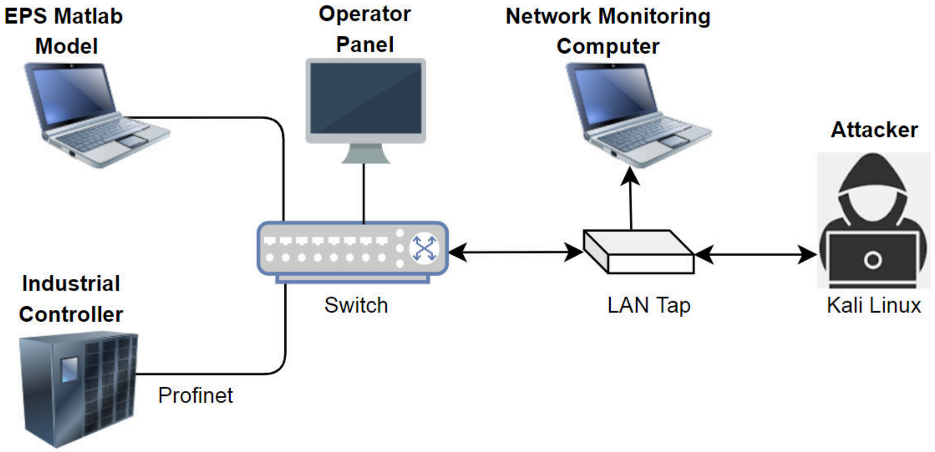

Fig. 8: Network Diagram for Attack Implementation and Network Monitoring

7 Experimental Analysis

An experimental result of an integrity attack using the hardware-in the loop setup is presented in this section. The target of this attack was the Circuit Breaker (CB) of a feed water pump, FWP1 of an NPP. An integrity attack is performed on the controller, controlling FWP1, by injecting false data configuration. The intention of this attack was to open the CB of FWP1 at an undesirable time. In Fig. 9, CB Status = 1 represents CB is closed and the FWP1 is running; CB Status = 0 represents CB is open and the FWP1 is disconnected from the power. Graph plotted in Fig. 9, is the representation of real time data received by Matlab/ Simulink model.

It can be noted from Fig. 9, at time t2 = 65 s, CB of FWP1 changed its status from 1 to 0. The alteration in the CB status was caused by the integrity attack that resulted in unintentional tripping of FWP1. The manipulated data configuration included overcurrent set-point parameter for the electric motor of a feed water pump in an NPP. This attack might also cause a healthy power line to become out-of-service even if there is no physical disturbance in power line.

Note: This threat scenarios was executed without considering the safety Instrumentation and Control (I&C) systems of an NPP. Therefore, only the operation I&C systems of the plant were targeted by leaving no impact on safety I&C systems.

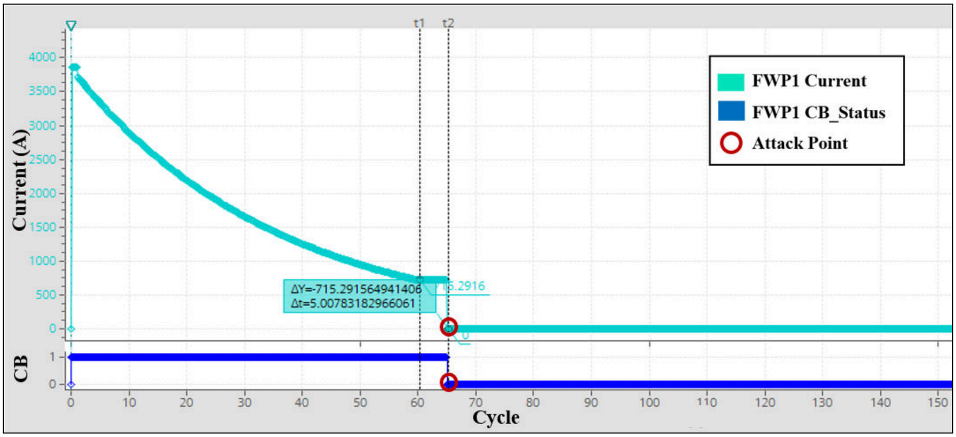

Fig. 9: Integrity Attack on FWP1 during Start-up Phase

8 Extension of the HIL Setup

The hardware in the loop setup presented in Section 6 can be further extended by an experimental model factory, operated by University of Applied Sciences Magdeburg Stendal [CB17] that has been modernized and expanded within the last years with regard to Industry 4.0. The model factory has been extended with common Siemens control (S7-1515F) and switches (Scalance SC615). Furthermore, a SIEM system was integrated. With this test setup, defined vulnerability tests are carried out and parameters are identified, which should enable an early detection of such attacks in the future.

With the structure described in Fig. 10 it is possible to model and experimentally evaluate attacks of different kinds [DI18]. The attacker system is a specially programmed framework or open source components. Thus, hidden channel attacks on different protocols or simple Denial of Service (DoS) attacks [SLD17] on different systems can be performed and analyzed.

As described in [SLD17] different attacks on PLCs could be evaluated and triggered. Thus disturbances, which are located on layer 2 and 3 of the OSI layer model, were tested by researchers. The disturbance caused by the test caused the blocking / isolation of the sensor signal, whereby the status change could no longer be transmitted to the control computer.

By integrating a manageable switch it is possible to implement virtual networks according to IEEE 802.1Q [IE14]. The segmentation resulting from the VLAN integration resulted in an increased protection against OSI Layer 2 and 3 attacks. However, this type of protection is only effective in conjunction with network segmentation.

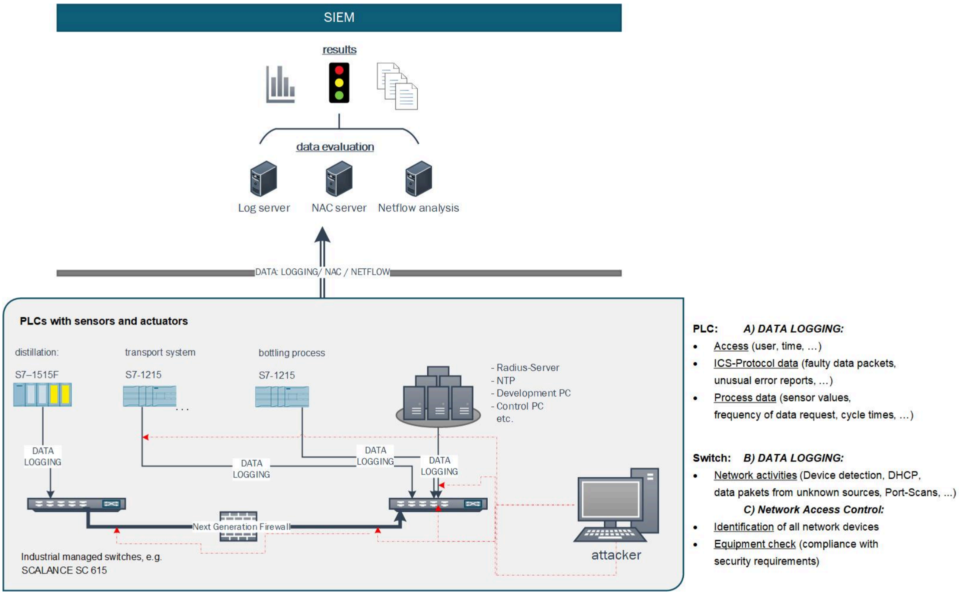
SIEM
results
data evaluation
Log server
NAC server
Netflow analysis
DATA LOGGING/ NAC / NETFLOW
PLCs with sensors and actuators
distillation:
S7–1515F
transport system
S7-1215
bottling process
S7-1215
- Radius-Server
- NTP
- Development PC
- Control PC
etc.
DATA LOGGING
DATA LOGGING
DATA LOGGING
DATA LOGGING
Next Generation Firewall
Industrial managed switches, e.g. SCALANCE SC 615
attacker
PLC: A) DATA LOGGING:
Access (user, time, ...)
ICS-Protocol data (faulty data packets, unusual error reports, ...)
Process data (sensor values, frequency of data request, cycle times, ...)
Switch: B) DATA LOGGING:
Network activities (Device detection, DHCP, data pakets from unknown sources, Port-Scans, ...)
C) Network Access Control:
Identification of all network devices
Equipment check (compliance with security requirements)

Fig. 10: Structure - Vulnerabilities Testing in an Experimental Environment

9 Summary and Outlook

The cyber-physical process model of targeted EPS inside a virtual NPP systems are described in this paper. The simulation model, divided in three parts (power generation, grid feed and house load) was designed and implemented using Matlab/ Simulink tool. The Simulink model was created to leverage freedom of customizing and testing of diverse threat scenarios. OPC UA communication protocol was used to setup the communication between Simulink model and physical devices. This simulation was used to analyze the impact of multiple cyber-threat scenarios by transferring the real time data from Simulink model to PLC and vice versa. A Network Diagram for cyber-attack implementation was also presented that was utilized to perform attack scenarios. An example integrity attack scenario was elaborated in this article. Furthermore, an extended version of the hardware in the loop setup – an experimental model factory was also presented in this paper that can be utilized for execution of more complex cyber-attacks and an early detection of such attacks in the future.

Acknowledgements

A part of our work in this domain is our contribution to IAEA project CRP J02008, entitled “Enhancing Computer Security Incident Response and Planning at Nuclear Facilities”. Some of the cybersecurity related topics are being elaborated as part of participation of Framatome

GmbH and University of Applied Sciences Magdeburg Stendal in the “SMARTEST” R&D (2015 - 2018) with German University partners, partially funded by German Ministry BMWi.

Bibliography

[CB17] Clausing, R,; Billowie, O.: Industrie 4.0 im Hochschul-Labor - Die Weiterentwicklung einer Modellfabrik. Tagungsband der Konferenz der Angewandten Automatisierungstechnik in Lehre und Entwicklung. Tagungsband - Angewandten Automatisierungstechnik in Lehre und Entwicklung (AALE), Wildau/Germany, 2017.

[DI20] DIN und DKE German Raodmap Industrie 4.0 Version 4, July 2020.

[DI18] Ding, Y.; Dittmann, J.; Szemkus, M; Lange, M.; Altschaffel, R.; Fischer, R.: Model-based vulnerability analysis of Complex infrastuctures, Berlin, 2018.

[IE14] IEEE Std 802.1, IEEE Standard for Local and Metropolitant Standard, Bridges and Bridged Network, Q. I. C. Society, 2014.

[IE10] IEC/TR 62541-2:2010 - OPC unified architecture - Part 2: Security model, 2010.

[Go19] Govindaraj, D.: Simulation of cybersecurity artefacts for Electrical Power Systems. Master Thesis, Darmstadt University of Applied Sciences, Germany, 2019.

[Gu20a] Gupta, D.: Nuclear Safety related Cybersecurity Impact Analysis and Security Posture Monitoring. PhD Thesis, Technical University Dresden, Germany, 2020.

[Gu20b] Gupta, D.; Govindaraj, D.; Altschaffel, R.; Waedt, K.: Blue Team Support for EPS Related Cybersecurity Readiness. In (ICONS 2020): IAEA International Conference on Nuclear Security, Vienna, 2020.

[Gu18] Gupta, D.; Bajramovic, E.; Parekh, M.; Waedt, K.: Threat Scenarios for Electrical Systems in Nuclear Power Plant. In (ICONE 2018): Proc. 26th International Conference on Nuclear Engineering, London, 2018.

[SLD17] Szemkus, M.; Lange, M.; Ding, Y.: IT-Security-Untersuchung an einer Modellfabrik unter Berücksichtigung der Industrie 4.0-Anforderungen. Tagungsband - Kommunikation in der Automation (KommA), Magdeburg, 2017.

[Ze11] Zeller, M.: Myth or reality does the aurora vulnerability pose a risk to my generator?, In (IEEE): Proc. 64th Annual Conference for Protective Relay Engineers, pp. 130–136, 2011.