

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

Deeksha Gupta¹, Yongjian Ding², Dharini Govindaraj³, Mathias Lange², Martin Szemkus², and Karl Waedt⁴

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 using transmission line and the distribution system connects the transmission system to the consumers. Cybersecurity issues for electrical power systems in transmission or in

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.d, 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

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 [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, False trip command, etc. However, the results of cyber-attack impact analysis are beyond the scope of this paper, only simulation model with physical process and communication is illustrated.

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 was used to setup the communication between the Simulink model and physical devices.

2 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).

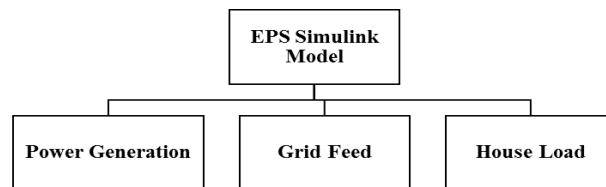


Fig. 1: Proposed EPS Model

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].

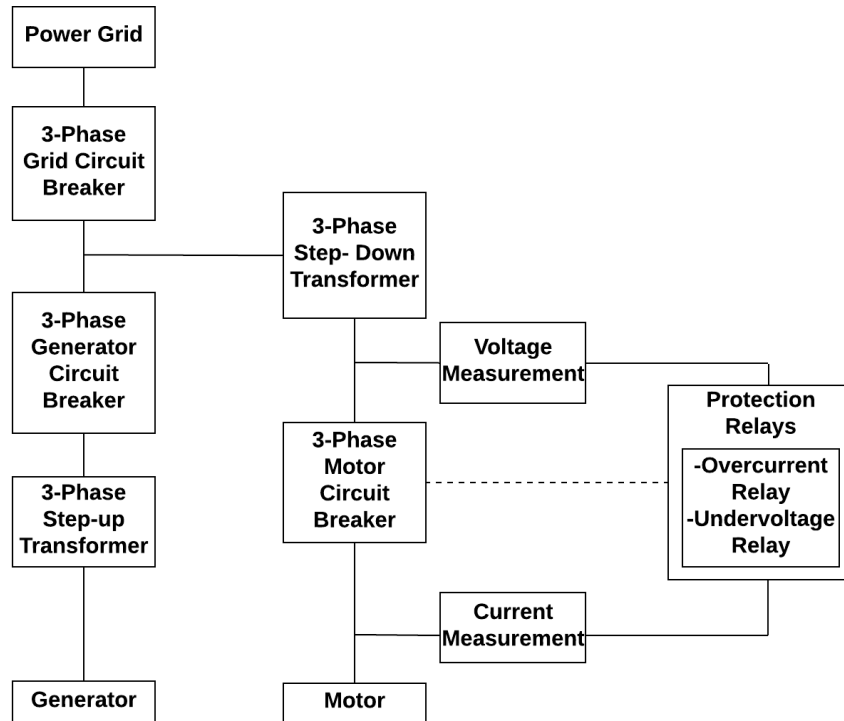


Fig. 2: Block diagram of EPS Simulink Model [Go19]

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:

- Synchronous Generator
- Step-up Transformer
- Circuit Breaker

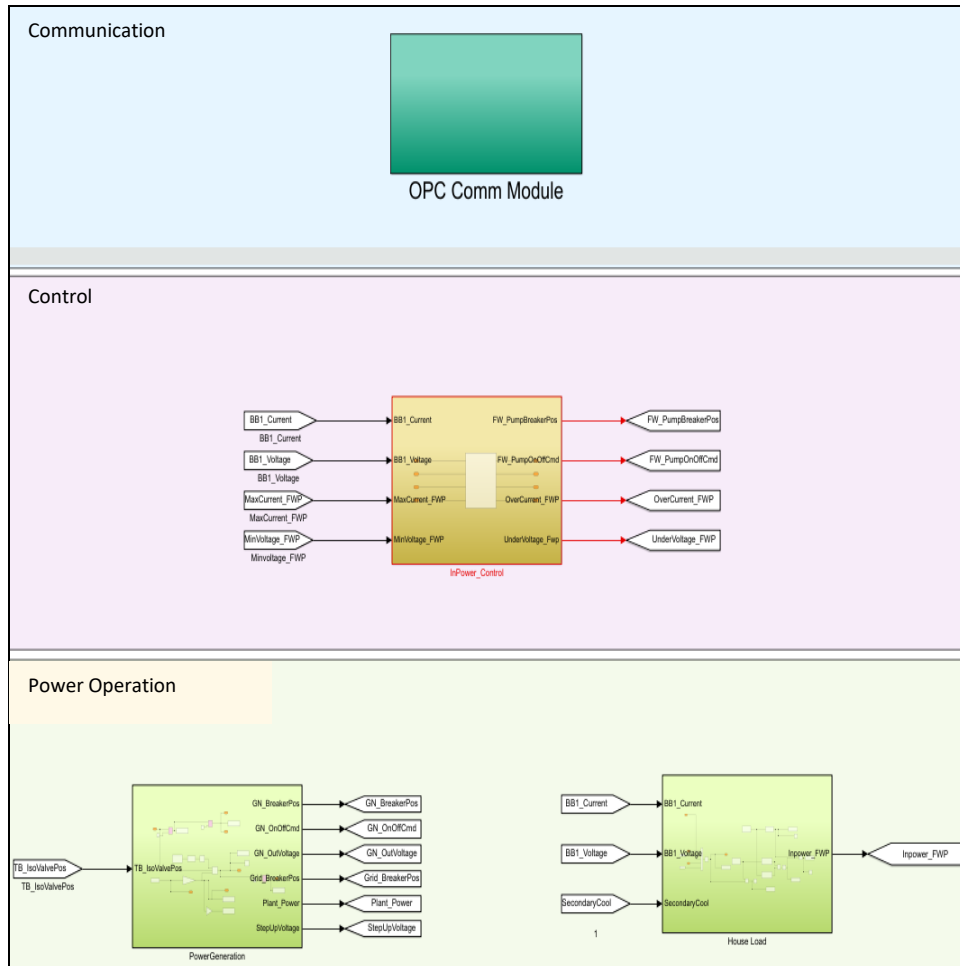


Fig. 3: Overview of MATLAB Simulink Model

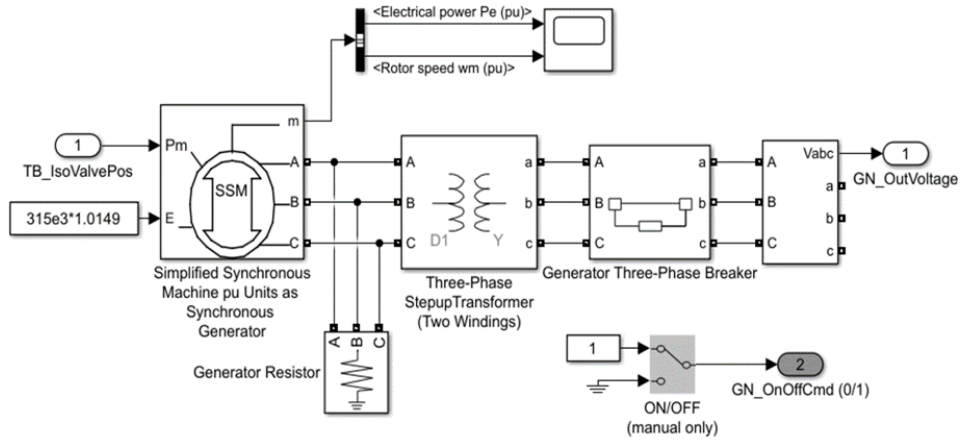


Fig. 4: Power Generation

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:

- Three-phase Source
- Transformer
- Three Phase
- PI Section Line and Series RLC load.

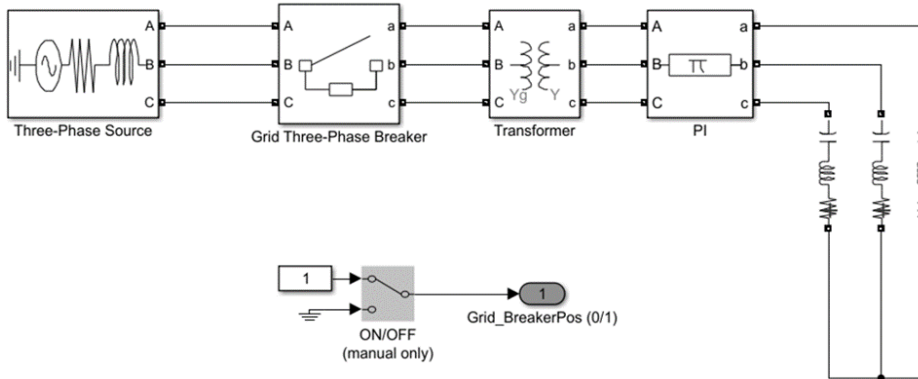


Fig. 5: Grid Feed Module

4.3 House Load

Fig. 6 shows the modelled house load module in Simulink model. This module has the following electrical components:

- Step-Down Transformer
- Circuit Breaker
- Asynchronous Motor
- Measurement Devices (current measurement and voltage measurement devices)
- Protection Devices for undervoltage and overcurrent protections

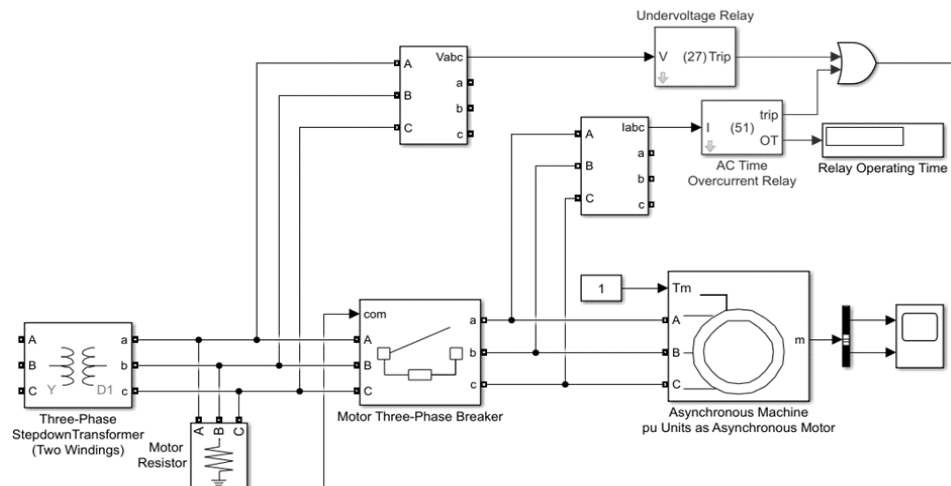


Fig. 6: House Load

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.

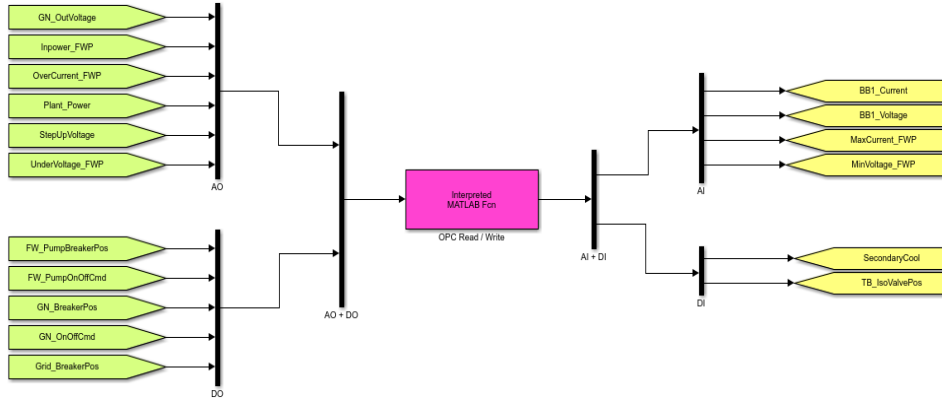


Fig. 7: OPC Tags for CommunicationTab. 1: OPC UA Tags Utilized in Simulink Model

<i>Tag Type</i>	<i>Tag Name</i>	<i>Significance</i>
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_PumpOnOffCmdStatus	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

Tab. 1: OPC UA Tags Utilized in Simulink Model

6 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.

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 Framatome GmbH’s participation in the “SMARTTEST” R&D (2015 - 2018) with German University partners, partially funded by German Ministry BMWi.

Bibliography

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