

Intelligent Micro Grid Controller Development for Hardware-in-the-loop Micro Grid Simulation Subject to Cyber-Attacks

Mike Mekkanen¹ Tero Vartiainen¹ Kimmo Kauhaniemi¹ Duong Dang¹

¹School of Technology and Innovation, University of Vaasa, Finland, {mike.mekkanen, tero.vartiainen, kimmo.kauhaniemi, duong.dang}@uwasa.fi

Abstract

This paper develops Hardware-in-the-loop (HIL) simulation against cyber attacks. We design a light-weight intelligent electronic device (IED) that performs Micro Grid Controller (MGC), interfaces are developed based on International Electrotechnical Commission (IEC) 61850 GOOSE protocol from/to the real-time simulation and the MGC. They are executed on two equipment stages, Field Programmable Gate Array (FPGA) and BeagleBoneBlack. CSIL versus CHIL tests are used to evaluate the Micro Grid (MG) behavior against different cyber attacks. We also evaluate the MGC designed control function in accordance with IEC 61850 GOOSE protocol. The results show that the light-weight MGC approach and data modeling of various IEC 61850 predefined data objects, data attributes and logical nodes (LNs) are correct for the design of the power balance control/protection function against cyber attacks in various cyber-attack case studies.

Keywords: Microgrid controller, co-simulation, EC61850, next-generation power system, real time simulator, cyber attack, HIL, IED.

1 Introduction

Renewable energy is considered as one of the solutions to stop global warming, and it has become the fastest-growing energy source in many countries (Dang et al., 2021; Eurostats, 2020). Due to the extensive integration interconnected of renewable plants (e.g., wind and solar) and other conventional generators (e.g., coal, oil), intelligent MGCs play very important roles in effectively controlling resources and loads that connect to MGs. For instance, in this study the developed MGC provides the power balance management between generation and consumption within the MG in a dynamic manner. Also, a controller can help to maintain the power balance of a medium voltage network within the limit settled by a distribution system operator.

Therefore, there is increasing interest in MGC's topics (Rajesh et al., 2017). For example, literature has focused on modelling, developing and implementing MG controllers (c.f., Colet-Subirachs et al., 2012; Li et

al., 2004; Ruiz-Alvarez et al., 2012; Sen and Kumar, 2018; Ustun et al., 2012; Zia et al., 2018). Also, pilot cases for various types of MG are studied by using early-stage MG controllers with vendor-defined characteristics (Liu et al., 2016). However, although MG standards have been published, the standardization of MG controllers is still under development (Sirviö et al., 2020). Based on the state of the art of standards and up-to-date products, it is argued that there are many issues related to MG controllers' product standards. For example, MG controllers' issues that are related to the interoperability of various systems and functions from different vendors (Baillieul et al., 2016; Reilly and Joos, 2018). Moreover, requirements for the MG controller at the point of interconnection (POI) are established by the standards (Reilly et al., 2017), in which the balance between power generations and loads consumptions (e.g., MG management) is one of the most important requirement for MG controllers that need to be acquired and offered. One possibility can be seen due to the requirements (set by the DSO) of power balance at the connected/Islanded MG situation under different circumstances (e.g., cyber-attack) in (Zhang et al., 2019). When developing and testing the operation of MG and MG controller functions, those issues should be taken into account. The test setup in Zhang et al., (2019), is based on the software-in-the-loop (SIL) MGC, however, the hardware-in-the-loop (HIL) testing is left for the developer.

Due to these issues, this research aims at developing a controller for MG HIL simulation against cyber-attacks. As a result, we develop MGC from a preliminary computing algorithm that needs to be implemented at a designed light-weight intelligent electronic device (IED). Interfaces are developed based on the IEC 61850 standard GOOSE protocol in the real-time simulation and test platform.

The paper is organized as follows. In Section 2 we illustrate the network development scenarios of the 25-kV medium voltage distribution network MG. Then, Section 3 presents the design light-weight IED with the preliminary power balance control algorithm, as well as IEC 61850 interfaces by libiec61850 library and C language. Next, Section 4 presents the MGC operation

within the CHIL simulations in the real-time simulation platform. The conclusions and discussions are presented in Section 5.

2 Development of MG and Testing Scenarios

A cutting-edge Real-Time Simulator (RTS) is a digital model-based test system that can precisely mimic the reaction of an actual physical system in real time. This digital replica of the actual physical system (digital twin) has been confirmed to be a valuable tool in power system research and studies for several decades. For example, a digital twin helps reduce test stresses on the actual physical system as well as hazardous work. Moreover, it enables the simulation model to interact with external hardware or control algorithms in such a way that external IED does not recognize that the received data is coming from a simulation model rather than actual physical system.

This work studies a MG 120kV grid-connected distribution feeder that can be islanded by opening the point of common coupling (PCC) circuit breaker and operating autonomously as developed in (Zhuang, 2012). The single line diagram of a MG and the cyber-physical structure are depicted in Figure 1. MG assets and their characteristics are depicted in Table 1.

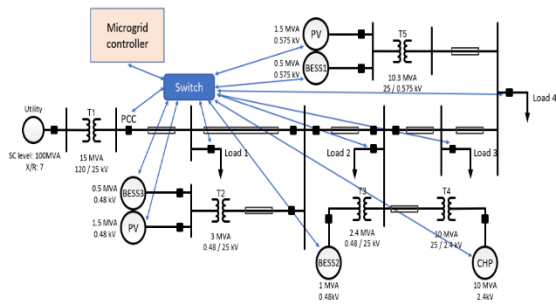


Figure 1: MG single line diagram and the cyber-physical structure, blue lines show the communication links that every MG node entity (DERs, loads, CB, etc.) send measurements, status to the MGC and received controlling signal from the MGC based on GOOSE IEC 61850 standard protocol.

Table 1 MG assets and loads

Asset	Type	Ratings	Operation Modes
Loads			
Load1	Critical	4MW	Always connected
Load2	Critical	4MW	Always connected
Load3	Hybrid	4MW	Can be disconnected on second priority
Load4	Non-Critical	3MW	To be disconnected

Asset	Type	Ratings	Operation Modes
in Islanded mode			
Distributed Energy Resources (DERs)			
Combined Heat and Power (CHP) plant	Gas Turbine	10MW	P/Q (Grid-connected) V/f (Grid forming)
2 x PV Generation System	With Smoothing Battery Energy Storage System	1.5MVA + 0.5MVA (1.2MWh)	MPPT with smoothing battery
3x Battery Energy Storage System (BESS)	Lead Acid	1MW (5MWh)	Power smoothing

The MG is a 25-kV medium voltage distribution network connected to a 120 kV sub-transmission system by means of a 15 MVA delta-wye transformer. The MG consists of 6 DERs, including two 1.5 MVA PV systems, three energy storage systems (ESS) (two of which are 500 kVA ESSs with 1.15 MWh capacity; one is a 1 MVA ESS with 5 MWh capacity), and one 10 MVA CHP unit. The MG also has four aggregated loads: the first two are critical loads rated at 4 MW, the third is a 4 MW priority load, and the fourth is a 5 MW non-critical load. The model does not include relay elements, which are beyond the scope of this study, there is no underlying protection scheme. Each MG asset is linked to a measurement subsystem, which is based on voltage and current measurements; a subsystem measurement component is programmed to produce P, Q, and V_{rms} measurements. These measurements from the measurement subsystems are sent to the MGC via IEC 61850.

We use the developed computing/controlling algorithm to extract and process those useful measurements from the received GOOSE messages within the MGC. The MGC is designed to provide power balance (calculates the total power generation and the total load consumptions) and manages the dispatch of the assets and load shedding of the non-critical load in the event of islanding. If the difference between the total power generation and the total load consumption exceeds 3MW for any MG actions or attacks, the controlling algorithm output (dispatching signal) will be sent back to the model via additional new GOOSE messages to shed off the non-critical load. In Zhang et al., (2019) simulates and tests a simple rule-based MGC on the same model using SIL. In contrast, in this paper, we use HIL to test the developed from scratch intelligent external MGC, which is left for the developer. We develop and run two scenarios to analyze/measure the MG behavior/resiliency of the MG

cyber-physical simulation against cyber attacks. In addition, we gain testing results for our developed MGC IED-based design computing algorithm and the MGC interfaces data model's compliance with the IEC 61850 standard.

2.1 Scenario 1: MG Islanding Operation Mode Against a delay attack on Load Shedding Trip

In the first scenario, the MG will be islanded in second 1, in this case the MGC will check the power balance and implement the power balance operation emergency condition (the difference not exceeds 3MW). If the check emergency condition becomes true, the MGC attempts to immediately disconnect the sheddable Load 4 to maintain the MG stability. Be that as a delay attack is introduced to the GOOSE trip command packets sent from the MGC to Load 4, the load shedding function may fail to operate in the required timeframe. In this case this will cause severe unbalance between generation/load relationship and oscillations on MG nominal operation parameters such as e.g., frequency, voltages etc. It may also result in severe consequences like a blackout. Through the C code available delay function within the MGC initial code, a one-second delay attack is applied to the MGC GOOSE message command. Secure Shell (SSH) terminal window is opened to control the MGC and monitor, record the MG physical system's reaction parameters. Wireshark network analyzer/sniffing tool is used for the same purpose, because the interfaces in the HIL test need to be implemented over a physical communication network, such as physical adapters, Ethernet switches, cables, etc.

2.2 Scenario 2: MG Steady State Islanded Operation Mode Against Man-in-the-Middle attack

MGC based on its normal operation will receive measurements that are sent from each MG assists via GOOSE. Be that as a Man-in-the-middle attack is introduced to the load measurements data. Before the load measurements data being received by MGC. The data is manipulated in the middle of its way to the MGC. In this case, the MGC may take incorrect actions based on these received non-critical measurements. According to the test scenario 2, the active power measurement from Load 2 is duplicated by applying a packet manipulation attack to the GOOSE message. In this case, the MGC will take the incorrect action (false tripping) because it perceives the controlling operation emergency condition is true (total load will be more than 3MW greater than the total generation). As a result, a trip command is sent to disconnect Load 3. It also

causes oscillations on MG nominal operation parameters such as e.g., frequency, voltages etc.

Comparison between both achieving testing results, SIL and HIL will be made within the rest of this work.

3 Design the light-weight MGC IED

The following describes the development process of the light-weight MGC that will be implemented as CHIL. The development process begins with the creation of an IEC 61850 Substation Configuration Description (SCL) file and its adaptation to two distinct hardware platforms: the BeagleBone Black (BBB) and the Field Programmable Gate Array (FPGA). The concept behind using these boards is based on their low cost, flexibility, support for various interfaces/protocols, I/O pins, and ease of configuration. Within the SCL file, we create the MGC object-oriented data model, which includes selected logical nodes (LN), data objects (DO), and data attributes (DA)s that are appropriate for handling and processing measurements data from the "field," in our case study, data come from the simulation model. In addition, we create and configure the GOOSE control blocks (GCB)s. To build the GCB, GOOSE datasets need to be created. This data set will include all the data attributes that need to be associated with the publishing of the MGC GOOSE messages. We finalize the GCB configuration by configuring the interfaces' GCB parameters such as GOOSE ID, GOOSE configuration revision, GOOSE publishing MAC address, GOOSE subscribing MAC address etc., as illustrated in Figure 2. In particular, the right side of Figure 2 shows the hierarchy structure of the developed MGC IED, including the communication IED section, list of the LNs, list of the GCBs and the list of the data sets. Whereas at the left side of Figure 3, it shows the list of the data attributes that includes the "OV2PTOV" GOOSE data set. These DAs will hold the measurements-status published from the DERs, loads and CBs, within the MG simulation model.

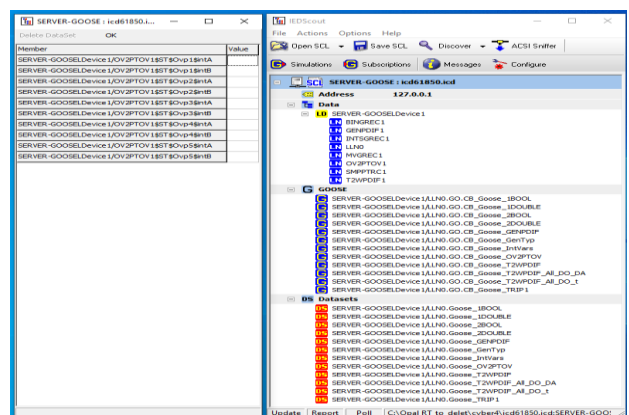


Figure 2. MGC SCL file

At this point the configured SCL file is used to create two files (static_model.c and static_model.h) by generating source codes (libiec61850, n.d., p. 61850).

The file `static_model.c` contains the definition of the data structures that build up the IED data model and also contains pre-configured values that are provided by the SCL file. The file `static_model.h` is intended to be included by the designed project code and defines handles that we can use for efficiently accessing the data model. According to the “model generator” process, each type of IED data model can be mapped directly to a C data structure, resulting in a hierarchy of C data structure. Besides, the generated C files must be accompanied by the platform-specific code to ensure consistency with IEC 61850. Consequently, MGC controlling power balance function in C language was developed in a way that complies with software-in-the-loop (SIL) preliminary algorithms developed by Opal HYPERSIM Power Systems [16].

The MGC controlling power balance function based on its operation, it needs to subscribe to the GOOSE messages that have been sent from the model with the associated measurements. After a successful subscription by the MGC, it needs to extract these measurements, and run the control function. At this point, the output of the control function based on the assigned emergency conditions that are explained earlier, are True or False. If it is True, the MGC needs to go to step, which is publishing a new GOOSE message that needs to be subscribed by the model. According to this GOOSE message an open CB command is sent. Then, it will return back to the previous step. Whereas, if the output is False, the MGC will send a heartbeat GOOSE messages without any changes. The procedure for designing the “lightweight” MGC HIL controller with all processing steps is presented in Figure 3.

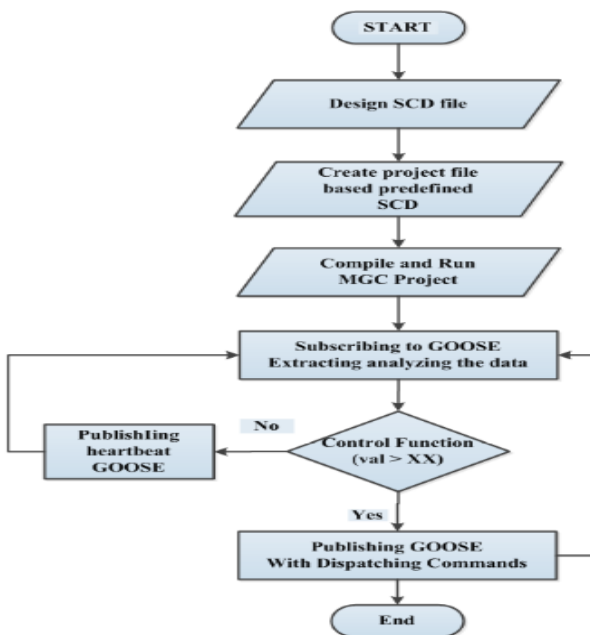


Figure 3: MGC development processing

The testing results will be presented in the next section of this manuscript.

4 CSIL and CHIL Testing Results

4.1 CSIL Testing Results

The workflow of the development of the real-time co-simulation platform consists of use cases development, closed-loop real-time simulations, light-weight MGC IED development, IEC61850 communication implementation, the CSIL, and the CHIL tests. At the beginning and according to the first CSIL scenario test, the MG power system is modeled and MGC is developed and both are implemented via Opal HYPERSIM software as illustrated in Figure 4 and Figure 5. Whereas, the IEC 61850 communication system is emulated in EXata software from Scalable as illustrated in Figure 1. Going into details of the HYPERSIM and EXata simulation/emulation models blocks/elements is out of the scope of this work.

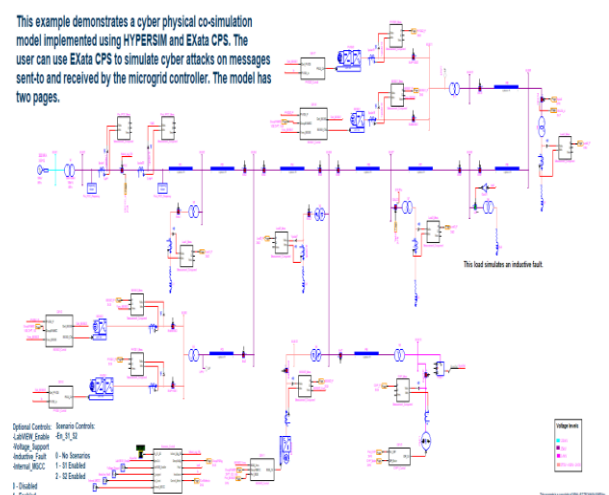


Figure 4. Opal HYPERSIM power system model

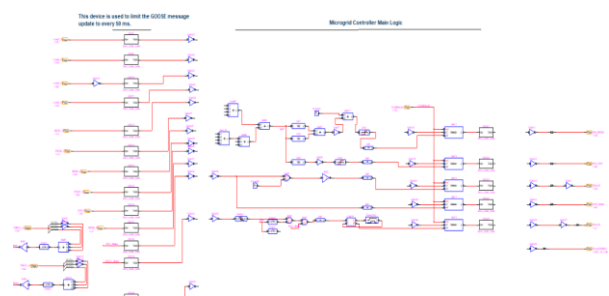


Figure 5. Opal HYPERSIM MGC model as SIL

As the MG goes to islanded mode after one second, the MGC sends a shedding command to load 4 via GOOSE messages in order to fulfill the emergency condition requirements. The results for the first case study are shown in Figure 6, MG returns to power balance after one second that appears in the upper part of Figure 6. Since we did not apply the delay attack yet as shown in the lower part of Figure 6, the sending and

receiving MGC single to shed load 4 is just an overlap which validates the fact that EXata is not adding more delay time within the communication system emulation and implementation.

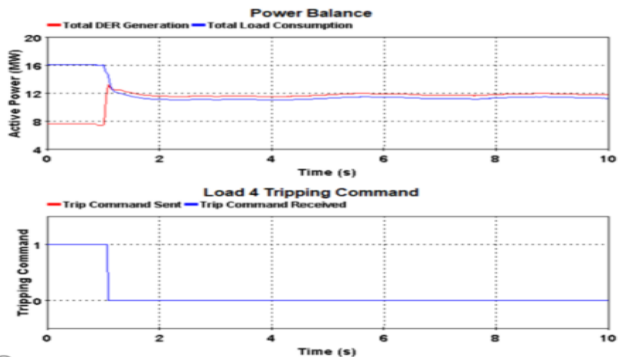


Figure 6. LabVIEW GUI in Opal HYPERSIM scenario 1 normal operation

Whereas, according to the second case study in the first scenario, we implement 1-second delay as a delay attack to MGC signal. Figure 7 illustrates the MG unbalance situation based on this attack, the MG took more time to return back to the balance mode as shown in the upper part of the figure. In the lower part of the figure, the MGC sends the trip command, however based on the attack it will be received by the IED that controls the load 4 CB after 1-second in which it affects the MG operation parameters such as f , V , power Quality, etc.

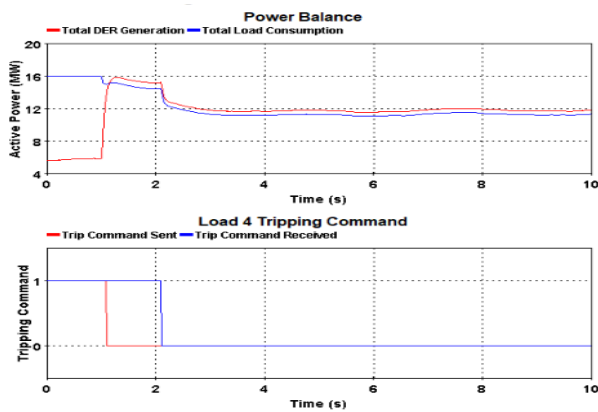


Figure 7. LabVIEW GUI in Opal HYPERSIM scenario 2 delay attack implemented to MG, lower figure shows the (red line) is the original trip signal sent from the MGC to shed off load 4 after the grid is islanded in second one, which it is in time. Whereas the (blue line) is the delayed signal. Trip command sent by the MGC is delayed by one second after we apply the cyber delay attack to the controller signal. Upper picture shows the MG unbalance operation that took a long period (more than 2 seconds).

According to the second scenario, the MG is islanded and in normal operation mode as illustrated in Figure 8. In the first case study, load 2 and load 3 are operated within their nominal operation values that consumes power around 4MW.

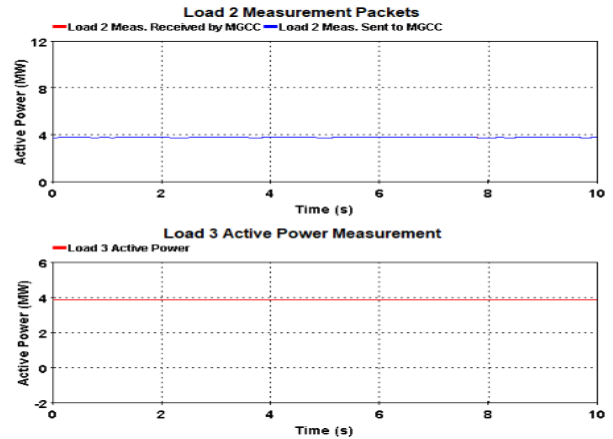


Figure 8. LabVIEW GUI in Opal HYPERSIM scenario 2 normal operation

Whereas, after applying the Man-in-the-middle attack to load 2 measurements in its way before it was received by the MGC. Figure 9 illustrates the load 2 measurements manipulation in which it doubled the load 2 power consumption (read curve) as shown in the upper part of the figure 9. In the lower part of the figure 9, it shows load 3 active power consumption that fluctuate between (0 - ≈ 4 MW) based on disconnecting and connecting modes, and the unbalance between the total power generation and total power consumption according to the attack. In addition, this situation also affects other MG operation parameters such as f , V , power quality, etc. that may lead to severe instrument damages or large blackouts.

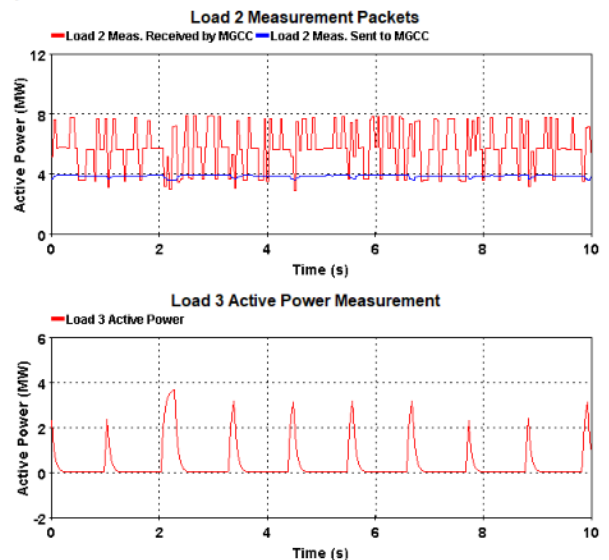


Figure 9. LabVIEW GUI in Opal HYPERSIM scenario 2 man-in-the-middle attack implemented to MG. Upper figure shows load 2 measurements (red curve) are manipulated before they are received by the MGC based on executing the man-in-the-middle attack, (blue curve) is the normal load 2 measurements before executing the attack. Lower figure shows the load 3 active power consumption which fluctuates between (0 and 4MW) since it is connected and disconnected to the grid based on executing the man-in-the-middle attack.

4.2 CHIL Testing Results

For the second part of this work, we show the HIL test and the testbed setup that is illustrated in Figure 10.

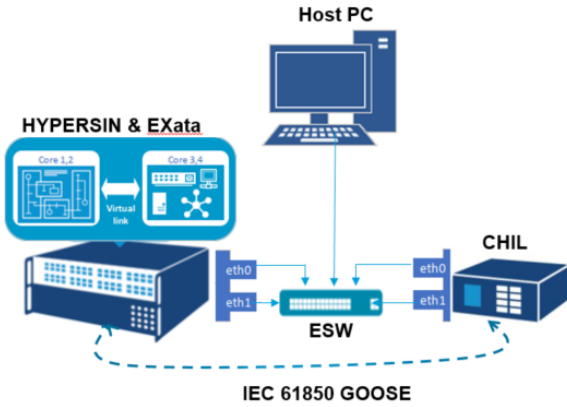


Figure 10. HIL testbed setup

According to the test setup principals, the light-weight MGC is developed that compliance with the IEC 61850 standard, the developed power system model within the HYPERSIM is upgraded and configured, in which the GOOSE publisher will use the physical adapter rather than the virtual adapter to publish the GOOSE messages over the designed communication network as illustrated in Figure 11. RJ45 cables are used to link the test instruments through the Ethernet switch.

#	SCL file	IED	GOOSE ID	Ethernet Adapter	Clock	AppID	MAC address
1	BESS1.CID	BESS1	BESS 1	eth0	INTERNAL	0x0002	01-0C-CD-01-00-02
2	PV.CID	PV	PV	eth0	INTERNAL	0x0003	01-0C-CD-01-00-03
3	BESS2.CID	BESS2	BESS 2	eth0	INTERNAL	0x0004	01-0C-CD-01-00-04
4	BESS3.CID	BESS3	BESS 3	eth0	INTERNAL	0x0005	01-0C-CD-01-00-05
5	PV2.CID	PV2	PV2	eth0	INTERNAL	0x0006	01-0C-CD-01-00-06
6	CHP.CID	CHP	CHP	eth0	INTERNAL	0x0009	01-0C-CD-01-00-09
7	PCC.CID	PCC	PCC status	eth0	INTERNAL	0x0008	01-0C-CD-01-00-08
8	Load1.CID	Load1	Load1	eth0	INTERNAL	0x0019	01-0C-CD-01-00-19
9	Load2.CID	Load2	Load2	eth0	INTERNAL	0x0010	01-0C-CD-01-00-10
10	Load3.CID	Load3	Load3	eth0	INTERNAL	0x0011	01-0C-CD-01-00-11
11	Load4.CID	Load4	Load4	eth0	INTERNAL	0x001E	01-0C-CD-01-00-1E
12	Load4.CID	Load4	Load4 status	eth0	INTERNAL	0x002D	01-0C-CD-01-00-2D
13	SEL_RTAC.CID	SEL_RTAC	DroopEMMGC	eth0	INTERNAL	0x0024	01-0C-CD-01-00-24
14	SEL_RTAC.CID	SEL_RTAC	BESS2 ref	eth0	INTERNAL	0x0027	01-0C-CD-01-00-27
15	SEL_RTAC.CID	SEL_RTAC	CHP ref	eth0	INTERNAL	0x002A	01-0C-CD-01-00-2A
16	SEL_RTAC.CID	SEL_RTAC	Load4 CB	eth0	INTERNAL	0x002E	01-0C-CD-01-00-2E
17	SEL_RTAC.CID	SEL_RTAC	CHP mode	eth0	INTERNAL	0x002F	01-0C-CD-01-00-2F
18	SEL_RTAC.CID	SEL_RTAC	Load3 CB	eth0	INTERNAL	0x0005	01-0C-CD-01-28-54
19	ico61850.scd	GOOSE-GOOSE	Goose OV2PTOV	eth0	INTERNAL	0x0005	01-0C-CD-01-28-54

Figure 11. Opal HYPERSIM I/O configuration

The light-weight MGC SSH terminal is used to execute and run the develop MGC project within the microcontroller boards based on Linux environment. Table 1 in Appendix, shows the MGC that has been successfully subscribed to the GOOSE messages published from the real-time simulator. In addition, it shows the tenth measurements that were extracted from the received GOOSE messages. All these extracted parameters are printed out to be shown on the output of the MGC control terminal. As well as, Wireshark sniffing tool is used to capture the GOOSE traffic and

also analyzes the tenth measurements associated within the captured GOOSE messages.

Different cyber attacks are implemented within the CHIL test procedure. The first case study is to measure the 1-second delay attack effects on the MG behavior. This delay attack is implemented within the MGC C code. While the second case study in order to simulate the Man-in-the-middle attack, we duplicate load 2 measurements by multiplying the measurements by two before sending it to the MGC. The MGC will extract the manipulated value from the attacked GOOSE message, and implement the check emergency condition in C code. In this case, MGC will send a dispatching command to disconnect load three to fulfill the emergency condition requirements. More analysis of the MGC GOOSE messages received data and discussion should be performed. Appendix Table 1 presents Scenario 1 CHIL data, which will be published as part of the study's continuation. Furthermore, different types of attacks, defender risk assessments, etc., will be tested in the future.

5 Conclusions

The development and performance of an MGC against cyber attack control schemes have been implemented in this paper. These are done by design and deployed on a light-weighted intelligent IED. The MGC control solution and its relevant communication system have been designed in compliance with the IEC 61850 and executed on two equipment stages, FPGA and BeagleBoneBlack. CSIL versus CHIL tests are used to evaluate/assess the MG behavior against different cyber attack scenarios. Moreover, we also evaluated IEC 61850 GOOSE protocol implementation, processing and finally control action performance. The obtained results demonstrate that the light-weight MGC approach and data modeling of various IEC 61850 predefined data object LNs are correct for the design of the power balance control/protection function against cyber attack. In addition, they demonstrate the successful implementations of the designed control/protection function and the modeled MGC LNs in various cyber-attack case studies on reliable detection of the emergency condition. Further work on the analysis of the data received by MGC, implementation of different cyber attacks and power balance detection algorithms is needed to validate the feasibility of the developed approach.

References

- Baillieul, J., Caramanis, M.C., Ilik, M.D., 2016. Control Challenges in Microgrids and the Role of Energy-Efficient Buildings. *Proceedings of the IEEE* 104 4 , 692–696. doi:10.1109/JPROC.2016.2532241
- Colet-Subirachs, A., Ruiz-Alvarez, A., Gomis-Bellmunt, O., Alvarez-Cuevas-Figuerola, F., Sudria-Andreu, A., 2012. Centralized and Distributed Active and Reactive Power Control of a Utility Connected Microgrid Using IEC61850. *IEEE Systems Journal* 6 1 , 58–67. doi:10.1109/JSYST.2011.2162924
- Dang, D., Vartiainen, T., Mekkanen, M., 2021. Towards Establishing Principles for Designing Cybersecurity Simulations of Cyber-Physical Artefacts in Real-Time Simulation. International Conference on Information Systems Development (ISD).
- Eurostats, 2020. Wind and water provide most renewable electricity [WWW Document]. URL <https://ec.europa.eu/eurostat/web/products-eurostat-news/-/ddn-20210108-1> (accessed 5.10.21).
- Li, Y., Vilathgamuwa, D.M., Loh, P.C., 2004. Design, analysis, and real-time testing of a controller for multibus microgrid system. *IEEE Transactions on Power Electronics* 19 5 , 1195–1204. doi:10.1109/TPEL.2004.833456
- libiec61850, n.d. libiec61850.
- Liu, G., Starke, M.R., Herron, A.N., 2016. *Microgrid Controller and Advanced Distribution Management System Survey Report* (No. ORNL/TM-2016/288). Oak Ridge National Lab. (ORNL), Oak Ridge, TN (United States). doi:10.2172/1287035
- opal-rt, n.d. Power system simulation and Power system Analysis (HYPERSIM). OPAL-RT. URL <https://www.opal-rt.com/systems-hypersim/> (accessed 5.10.21).
- Rajesh, K.S., Dash, S.S., Rajagopal, R., Sridhar, R., 2017. A review on control of ac microgrid. *Renewable and Sustainable Energy Reviews* 71, 814–819. doi:10.1016/j.rser.2016.12.106
- Reilly, J., Hefner, A., Marchionini, B., Joos, G., 2017. *Microgrid Controller Standardization: Approach, Benefits and Implementation*. Cleveland, OH.
- Reilly, J., Joos, G., 2018. Microgrid Controller Standards for Integration and Interoperability. Presented at the CIRED 2018 Ljubljana Workshop on Microgrids and Local Energy Communities, AIM. doi:10.34890/64
- Dang, D., Vartiainen, T., 2020. Changing Patterns in the Process of Digital Transformation Initiative in Established Firms: The Case of an Energy Sector Company. PACIS 2020 Proceedings.
- Ruiz-Alvarez, A., Colet-Subirachs, A., Alvarez-Cuevas Figuerola, F., Gomis-Bellmunt, O., Sudria-Andreu, A., 2012. Operation of a Utility Connected Microgrid Using an IEC 61850-Based Multi-Level Management System. *IEEE Transactions on Smart Grid* 3 2 , 858–865. doi:10.1109/TSG.2012.2187222
- Sen, S., Kumar, V., 2018. Microgrid control: A comprehensive survey. *Annual Reviews in Control* 45, 118–151. doi:10.1016/j.arcontrol.2018.04.012
- Sirviö, K.H., Mekkanen, M., Kauhaniemi, K., Laaksonen, H., Salo, A., Castro, F., Babazadeh, D., 2020. Accelerated Real-Time Simulations for Testing a Reactive Power Flow Controller in Long-Term Case Studies. *Journal of Electrical and Computer Engineering* 2020, e8265373. doi:10.1155/2020/8265373
- Ustun, T.S., Ozansoy, C., Zayegh, A., 2012. Modeling of a Centralized Microgrid Protection System and Distributed Energy Resources According to IEC 61850-7-420. *IEEE Transactions on Power Systems* 27 3 , 1560–1567. doi:10.1109/TPWRS.2012.2185072
- Zhang, L., Li, S., Wihl, L., Kazemtabrizi, M., Ali, S.Q., Paquin, J.-N., Labbé, S., 2019. *Cybersecurity Study of Power System Utilizing Advanced CPS Simulation Tools*. White paper, OPAL 13.
- Zhuang, D., 2012. *Real time testing of intelligent relays for synchronous distributed generation islanding detection*. McGill University, Montréal, Québec, Canada.
- Zia, M.F., Elbouchikhi, E., Benbouzid, M., 2018. Microgrids energy management systems: A critical review on methods, solutions, and prospects. *Applied Energy* 222, 1033–1055. doi:10.1016/j.apenergy.2018.04.103

