Modelica-Supported Attack Impact Evaluation in Cyber Physical Energy System

Kaikai Pan†, Digvijay Gusain, Peter Palensky
Department of Electrical Sustainable Energy
Faculty of EEMCS, Delft University of Technology
Delft, The Netherlands
Email: k.pan@tudelft.nl

***Abstract*—The evolved smart grid has become a cyber physical energy system that could be exposed to a massive amount of cyber threats. Vulnerabilities within the cyber part can be used to launch multiple types of attacks that corrupt the physical system. The complexity of cyber physical energy system, the existing of different kinds of attacks, require an appropriate tool to aid in modeling and simulation for cyber security analysis. In this paper, we introduce a modeling language - Modelica to the security community of cyber physical system. We show the capability of Modelica in modeling complex systems and attacks by building up a power grid model with frequency control loop (i.e., automatic generation control), as well as data integrity attack and data availability attack models. The simulation results show how different types of attacks or even combined attacks can affect the system frequency stability.**

I. Introduction

The integration of physical power systems, automated devices, digitalized controls, and widespread information and communication technology (ICT) components gives the smart grid a character of the cyber physical energy system (CPES). Such a combination of a physical system with ICT may lead to many dependencies that require attention. One important aspect is the cyber security analysis. Vulnerabilities within ICT components have made CPES exposed to a large number of cyber attacks; see [1], [2] for real examples. To make the situation worse, such cyber threats allow an attacker to manipulate the physical system directly, which may bring disastrous economic and humanitarian consequences.

We would like to refer to the secondary frequency control process in the smart grid as an instance of such dependency: an Automatic Generation Control (AGC) block collects the measurements from remote sensors and sends back generation control commands to the participating generators to restore the frequency to its nominal values and maintain the tie-line power flows between authority areas [3]. However, these measurements and control data are commonly transmitted through unprotected Supervisory Control and Data Acquisition (SCADA) networks. Manipulation of the measurements or control commands can cause catastrophic consequences from frequency deviations to equipment damages and cascading failures. The critical nature of AGC highlights the importance of making it secure to the power grid operation. To increase the security of this process, one needs appropriate methods or tools to assess the attack impact. Some of the literature has already tackled this problem. Analytic analysis of attack impact on AGC has been performed in [4] using a reachability framework. Experimental results were shown in [5] where AGC was attacked by false data injection (FDI) attacks. Other work has also been conducted on how an optimal attack can cause the most damages [3], [6], while again, most of the literature focuses only on the pure type of data integrity attack, i.e., FDI attack.

Except for analytic methods, appropriate tools with the capability of modeling CPSE and cyber attacks are desired. The increasing nature of the CPSE requires rethinking of the modeling language. However, developing a suitable modeling language for simulating complex CPSE remains challenging [7]. Modelica, as a unified language supporting multi-domain physical systems modeling and hybrid continuous/discrete systems modeling, has shown its great potentiality in modeling and simulation of CPES. In this paper, we aim to contribute in facilitating the employment of Modelica in analyzing the behavior of CPES under adversarial attacks. We take the AGC process under different types of attacks as an instance. Besides, instead of pure data integrity attack, we extend the attack scenarios to include the data availability attack and even a combination of data integrity and availability attack. Different case studies of attacks would be conducted within OpenModelica (an open-source Modelica-based modeling software), and the attack impact can be evaluated.

Section II details the problem statement and our motivations for modeling and simulation of cyber attacks in CPES. In Section III, we provide the basics of the modeling instance: attacks on the frequency control loop (i.e., AGC) of the power grid. The strategies of FDI attacks, data availability attacks, or even combined attacks are illustrated. The modeling description in Modelica is presented in Section IV, in which we show how the physical system, control loop and different types of attacks are modeled. Section V shows the numerical results of attack impact simulated in OpenModelica, while the conclusion remarks are given in Section VI.

II. Problem Statement and Motivation

A. Cyber Physical Energy System Under Attacks

A type of CPES can be spatially distributed system where the physical plant is operated by digital controllers that receive measurements from remote sensors and send back control

commands to the actuators through an ICT network (e.g., SCADA); see [8]. Here we denote the measurements as $y \in \mathbb{R}^{n_y}$, while the control commands correspond to $u \in \mathbb{R}^{n_u}$. The measurements and control data are transmitted through the communication network to be delivered in time. However, as mentioned above, the ICT networks are potentially vulnerable to cyber threats. Spatially distributed CPES needs remote access connections for monitoring and maintenance, which may expose them to cyber attacks. For most industrial communication protocols, e.g., DNP 3.0, IEC 61850, adequate security features were not always equipped at the time of publishing [9]. This motivates us to develop appropriate tools to analyze cyber attacks.

An adversary could gain access to the measurements and control signals by tampering with the ICT network. From the side of the CPES, the received measurements and control data would be corrupted to $\tilde{y}$ and $\tilde{u}$. The corrupted $\tilde{y}$ and $\tilde{u}$ under different types of attacks can be represented as follows,

- Data integrity attack - known as FDI attack, is able to change the measurements or control signals to $\tilde{y} = y + a_y$ and $\tilde{u} = u + a_u$ where $a_y \in \mathbb{R}^{n_y}$ and $a_u \in \mathbb{R}^{n_u}$ are the corruptions. Here we omit other types of data integrity attacks such as replay attacks since they can be modeled as FDI attacks eventually.
- Data availability attack - includes denial of service (DoS) attack which would prevent the data from reaching their respective destinations. One typical scheme used by digital controllers to deal with unavailable data is to replace the absent data with the last received data [10]. Thus $\tilde{y} = y_\tau$ and $\tilde{u} = u_\tau$ where $y_\tau \in \mathbb{R}^{n_y}$ and $u_\tau \in \mathbb{R}^{n_u}$ are the last received data.
- Combined attack - an advanced attacker would use all the available tools to launch both data integrity and availability attacks. From [11] we proposed combined attack scenarios on measurements data, i.e., $\tilde{y} = (I - \mathrm{diag}(d_y))y + a_y$ where $d_y \in \{0,1\}^{n_y}$ denote the availability attack and I is an identity matrix. More complex cases could be combined attacks on both measurements and control signals, leading to different possible combinations.

B. Towards Secure Cyber Physical Energy System

To support the security analysis of CPES, there has been a considerable amount of work based on analytic methods [3], [4], [8], [12]. These system-theoretic measures usually describe the energy system entirely by differential algebraic equations. Besides, most of them focus on pure type of attack, i.e., FDI attack, while the attack scenario can be significantly complex when it comes to combined attacks. This would make a system-theoretic description of the CPES under different types of attacks even impossible. Thus tools for modeling and simulation of CPES under attacks are needed.

However, based on the prior discussion, it is evident that the coupling of the physical system with various other heterogeneous systems in CPES can be of an entirely different nature, which opens a wide range of opportunities, but at the same time comes with challenges in the modeling and simulation

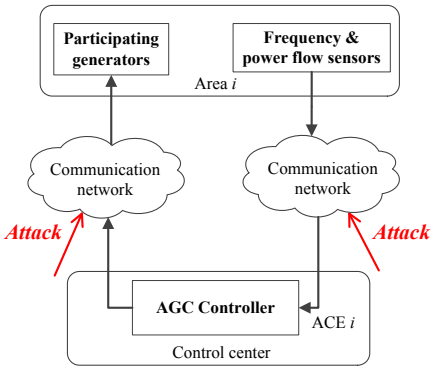

Figure 1. The model of AGC system for Area i.

[13]. Modeling a CPES under attacks should consider the following features:

- Distributed sensing, actuation, control can be modeled and simulated in an easy way [14].
- The interoperability of the various models (e.g., control, ICT, physical system) requires specified interfaces.
- It should include the capability of hybrid continuous and discrete modeling, as well as attack modeling.

Modelica is one of the most promising modeling languages that can facilitate the integrated modeling and simulation of CPES; see Section IV for details. Thus in this paper, we are motivated to introduce Modelica for cybersecurity community within cyber physical systems. We would present a modeling framework that allows simulation of CPES in OpenModelica under different attack scenarios.

III. Attacks on Automatic Generation Control of CPES

A. Basics of Automatic Generation Control System

AGC is the automatic closed-loop that regulates power grid frequency by tuning the setpoints of the generators. As shown in Figure 1, for a distributed multi-area energy system, the AGC block in each area collects the frequency and tie-line power flow measurements and sends back control signals to the participating generators, through SCADA network mostly with DNP 3.0 protocol. After receiving measurements, the control center in area i calculates an area control error (ACE) signal:

$$ACE_i = \beta_i(f_i - f_0) + (P_{tie_i} - P_{tie_0}), \tag{1}$$

where β_i is the frequency bias, f_i and $Ptie_i$ denote the frequency and power flow measurements in area i, and f_0 and P_{tie_0} correspond to the nominal values. The ACE value defines the power to compensate and the frequency to restore in the event of imbalance between generation and consumption in area i. With the input of ACE_i, the AGC controller generates an output control signal for the participating generator to track the load changes. This is usually a proportional–integral (PI) controller which can be expressed in s domain:

$$\Delta P_{agc_i} = (K_{P_i} + \frac{K_{I_i}}{s})ACE_i, \tag{2}$$

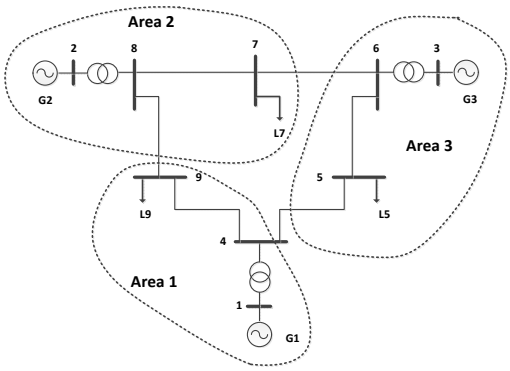

Figure 2. IEEE 9 bus system in 3 areas. Each area is equipped with AGC system.

where K_{P_i} and K_{I_i} are the coefficients of the proportional and integral terms for AGC block in area i, and ΔP_{agc_i} represents the AGC output signal that is feeding into the governor of the generator. In the work of analytic analysis of AGC, usually, each area of a power grid is represented by a linearized model comprised of equivalent governors, turbines and generators. With the linearized model together with Equation (1) and Equation (2), a state-space based representation can be derived. We refer to [4] for details. However, this linearized model lacks essential details compared to a full system model, which can provide greater insights into dynamic behavior of the system. For a more accurate and realistic analysis of cyber attacks against AGC, in this paper, we would model a fully detailed IEEE benchmark system (Figure 2).

B. Attack Scenarios Against AGC

In Figure 1, attackers can intrude the susceptible communication channels on both measurements and control signals. The potential attack targets include 1) frequency; 2) exported power flows; 3) AGC controller outputs. Different from the majority of the work with an emphasis on FDI attack, in this paper, both FDI attack and data availability attack or even combined attack would be considered. To be noted, we focus on the three-area 9 bus system where one area is attacked.

1) FDI attacks on frequency or power flow measurements: Attacker in this case would introduce an injection on the frequency or power flow measurements in area i. For both cases, the corrupted $ACE_{i,a}$ can be expressed as a combination of the ture ACE_i and the corruption term a_i:

$$ACE_{i,a} = ACE_i + a_i. \tag{3}$$

It has been proved in [15] that when the data injection $a > 0$, then it renders the frequency after corruption f_a smaller than the nominal value f_0. Inversely when $a < 0$, it renders $f_a > f_0$.

2) FDI attacks on AGC control outputs: Attacker will change the AGC controller output signal, such that the received AGC output would be injected with an additive signal a_0,

$$\Delta P_{agc_{i,a}} = \Delta P_{agc_i} + a_0. \tag{4}$$

For this type of FDI attack on AGC outputs, the corrupted frequency would increase first if $a_0 > 0$ since the generator is enforced to produce more power, while the frequency decreases if $a_0 < 0$.

3) DoS attacks on frequency or power flow measurements: According to the strategy discussed in Section II-A, the AGC controller would use the last received measurements, i.e.,

$$ACE_{i,d} = ACE_{i,\tau}, \tag{5}$$

where $ACE_{i,\tau}$ is the last normal ACE value. To make the data availability attack "effective", let us introduce a load event such that the load has increased while an availability attack has been launched simultaneously. The generator will act as if there is no AGC in area i, resulting in a drop of frequency and stabilization only using the governor of area i.

4) DoS attacks on AGC outputs: Similar to the previous case, the generator continues to use the last received normal AGC controller signal, i.e.,

$$\Delta P_{agc_{i,d}} = \Delta P_{agc_{i,\tau}}, \tag{6}$$

where $\Delta P_{agc_{i,\tau}}$ is the last received AGC output signal. We can still consider the same load event in area i, and again this would make the frequency drops due to the load increase event.

5) Combined data integrity and availability attacks: This makes the situation much more complicated that there exist several possible combinations. For instance, the measurements would be blocked by a DoS attack while the AGC outputs are injected with false data. The AGC controller could be disrupted that the system is damaged. From the other point, the state-space based model cannot be enough for analyzing such complex attacks scenarios. An appropriate tool is needed with such capability, which would be addressed in Section IV using Modelica.

IV. Modelica-based CPES and Attack Modeling

Modelica is an object-oriented, multi-domain modeling language that can be used in modeling of complex systems, such as, systems containing mechanical, electrical, electronic, hydraulic, thermal, control, electric power or process-oriented sub-components. This is achieved by inherent modeling philosophy that Modelica adopts. Connections (interfaces) can be defined as physical quantities (in terms of potential and flow variables) or signals (Real, Integer or Boolean, etc.). This enables accurate modeling of physical, continuous systems, as well as discrete systems such as communications systems. This allows modeling of a hybrid CPES, which represents a system that is closer to reality.

A. Network Model Description

In this study, we modeled an IEEE 9 bus system using the OpenIPSL library [16] in OpenModelica. The system is illustrated in Figure 3. The network consists of 9 buses, 3 generators, 3 two-winding power transformers, 6 lines and 3 loads, representing a 3-area transmission network.

The dynamic generator model consists of a fourth order synchronous machine, along with automatic voltage regulator (AVR) and turbine governor model (GOV). These controllers are part of all three generators in the test case. AVR helps with

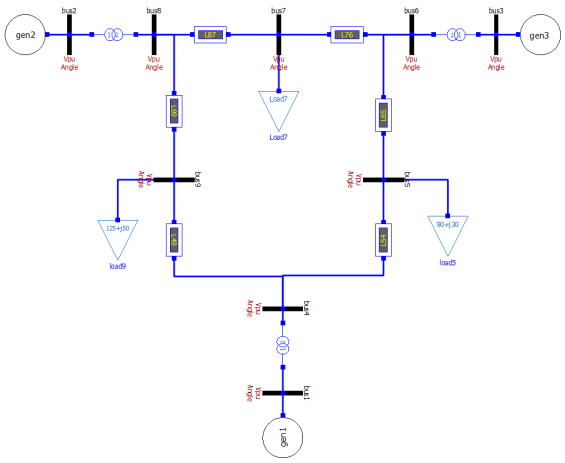

Figure 3. The IEEE 9 bus system modelled in OpenModelica

regulating the voltage of the system by changing field winding voltage. As mentioned earlier, the governor is used to regulate initial frequency variations. It helps the generator to reduce the frequency deviation by increasing power production.

According to Figure 2, the 9-bus network is divided into three areas, each consisting of a generator and a load. Transmission lines called tie lines connect areas. Each area has its own AGC controller to regulate the frequency of each area and the tie-line power flows. The AGC is modeled as a PI controller as shown in Figure 4. It collects the measurements of frequency and power flows exported from that area. The AGC controller then uses these measurements to calculate the ACE as explained in Section III-A. In the real world case, the inputs to the AGC with relevant information is delivered at specific time intervals. The calculated mechanical power setpoints (i.e., the AGC output signals) are then delivered to the participating generators. The data of measurements and setpoints are transmitted through a communication network which typically involves communication delays. In this paper, we are mainly focusing on the modeling of the physical power network, controllers and attacks that we assume an ideal communication. Libraries for modeling discrete-event based communication network are referred to [17].

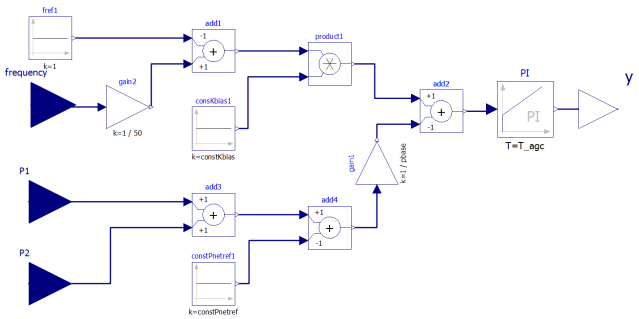

Figure 4. Model of AGC in OpenModelica

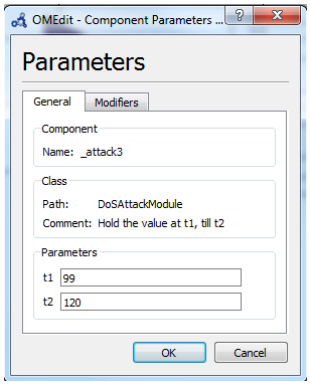

Figure 5. Setting up DoS attack in OpenModelica

B. Attack Modelling

As mentioned in Section II-A and Section III-B, the network undergoes three types of cyber attacks. For this study, new attack models were created in OpenModelica to simulate the listed attack scenarios.

- The FDI attack is simulated by a block which adds a step input to the existing measurement/control signal before giving it to the AGC controller/machine governor. Users can specify the time of the attack and the attack intensity.
- The DoS attack is simulated by another block which does not update the measurements/control signal to the AGC controller/machine governor for a user-defined time interval. This model follows the algorithm as shown in Section III-B.
- The combined attack is simulated by using the above-mentioned blocks together.

All these three attack modules were modeled using Modelica Standard Library in OpenModelica.

The system model with attack modules is shown in Figure 6. The green blocks are AGC controllers that accept frequency and power flows at interconnections to two other areas. The component in red is a DoS attack module. The component in blue is the model for FDI attack. In Figure 6, the electrical network block is a representation of network in Figure 3.

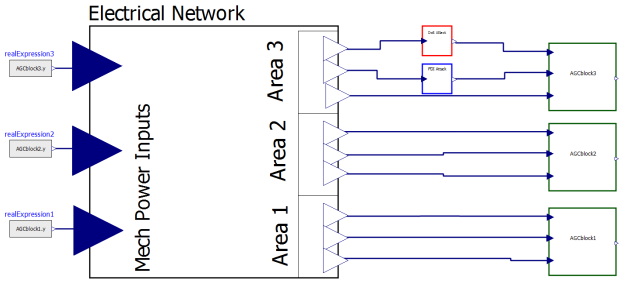

Figure 6. Complete network model with all attack modules in OpenModelica.

V. Simulation Results

In this section, simulations are performed to evaluate the impact of the aforementioned attack strategies(i.e., FDI attack,

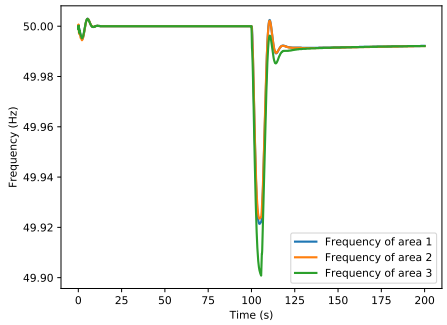

Figure 7. Frequencies of each area in 9 bus system under FDI attack on power flow measurement of area 3.

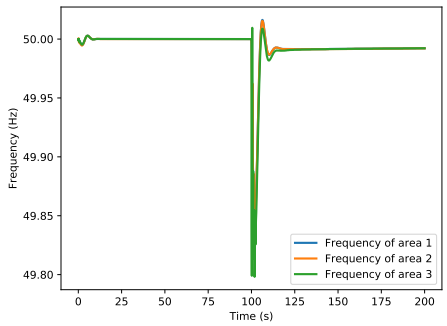

Figure 8. Frequencies of each area in 9 bus system under FDI attack on AGC output of area 3.

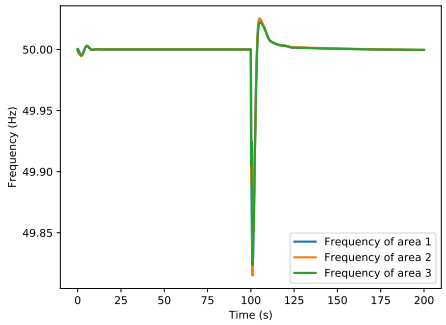

Figure 9. Frequencies of each area in 9 bus system under DoS attack on power flow measurement. There is a load event in area 2.

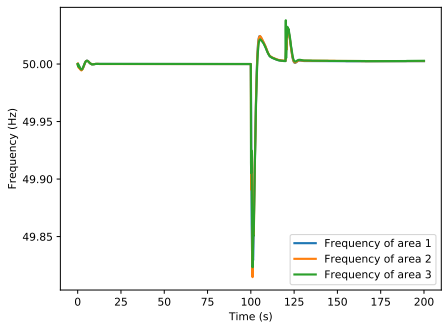

Figure 10. Frequencies of each area in 9 bus system under DoS attack on AGC output of area3. There is a load event in area 2.

DoS attack, combined attack) on the AGC performance. The 3-area IEEE 9 bus system in Figure 2 is used as the test case. The attacker compromises the measurements and/or AGC outputs in area 3 while area 1 and area 2 are intact. The 9 bus system, AGC controller and the attack models are implemented in OpenModelica as described in Section IV.

1) FDI Attack Results: In this simulation case, the AGC control system is operating normally at the beginning. The total power generation and consumption keep balanced. At time 100 s, the FDI attack occurs on the measurements or AGC controller outputs. Figure 7 and Figure 8 shows the simulation results of FDI attacks on power flow measurement and AGC output control signal, respectively. In Figure 7, the attacker injected a positive term to the ACE_3, i.e., $a_3 > 0$ in Equation (3), rendering the frequency after attack smaller than the normal value 50 Hz. The results of an FDI attack on AGC output ΔP_{agc_3} are shown in Figure 8, in which the injected signal follows $a_0 < 0$. This makes the generator in area 3 decrease the power generation, and the frequency drops below the nominal value. These results prove that FDI attacks on measurements or AGC outputs can directly cause deviations of system frequency, disrupting the stability of the system.

1) Data Availability Attack Results: To see the impact of data availability attack on AGC system, we added a load event for the system while a DoS attack was launched. At time 100 s, a load event happens in area 2 that the load consumption has increased by 50 %. Figure 7 and Figure 8 shows the simulation results of DoS attacks on power flow measurement and AGC output signal. In both cases, the DoS attack occurs at 100 s and stops at 120 s. Note that the DoS attack was launched in area 3. As shown in Figure 7, the frequency of each area behaves normally as the one under load event that the AGC controls succeed to restore the frequency to the nominal values. This is because the AGC controls of area 1 and area 2 are working perfectly to remain the power flow between area 1/area 2 and area 3, while the AGC control of area 3 uses the last received normal power flow measurement. In Figure 8, the DoS attack happens in the AGC output of area 3. The frequency of each area can still be restored to the nominal values after the DoS attack, though it takes a longer period to drive the system back to the steady state. This means the AGC controllers in this 3-area 9 bus system can withstand a certain level of DoS attack if it happens only in area 3.

1) Combined Attack Results: As it has been mentioned, the attack scenarios can be so complex that the evaluation of the attack impact has to be based on simulations instead of analytic methods. To compare the results of combined attacks with pure type attacks, we considered two attack scenarios: a) An FDI attack corrupts the power flow measurement of area 3. This corruption is the same with the pure FDI attack as before. At

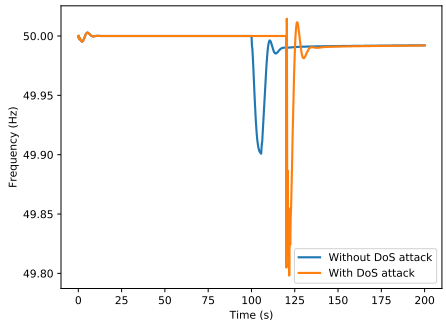

Figure 11. Frequencies of each area in 9 bus system under combined attacks. The FDI attack corrupts power flow measurement of area 3 while the DoS attack corrupts the AGC output of area 3.

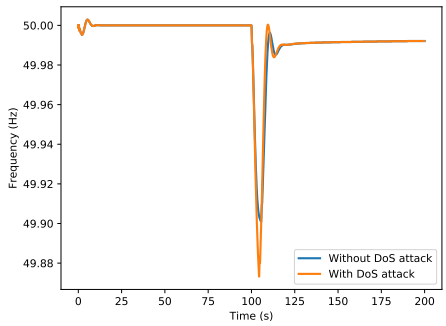

Figure 12. Frequencies of each area in 9 bus system under combined attacks. The FDI attack corrupts power flow measurement of area 3 while the DoS attack corrupts the frequency measurement of area 3.

the same time, a DoS attack is launched in the AGC output signal of area 3. b) An FDI attack still corrupts the power flow measurement of area 3, but the DoS attack is launched on the frequency measurement of area 3 that it is blocked from 100 s to 120 s. Figure 7 and Figure 8 shows the simulation results for these two cases correspondingly. As shown in Figure 7, though the frequency can keep normal from 100 s to 120 s because the DoS attack "delayed" the impact of the FDI attack, the damage is becoming more severe in the case of combined attacks. In Figure 8, the combined attacks take places on the measurements side. Comparing to the pure FDI attacks, again the combined attacks lead to greater frequency drops. This is due to the fact that the AGC controller cannot track the frequency changes owing to the DoS attack. Therefore, combined attacks can cause severe damages by driving the system into large oscillations. Attention should be paid to combined attacks, and protection schemes are required to mitigate the impact of combined attacks.

VI. Conclusion

In this paper, we contribute to introducing Modelica for supporting cybersecurity analysis in CPES. The results show the capability of Modelica in modeling complex system under different types of attacks. We use the instance of attacks on the frequency control loop in the power grid to explore the impact of attacks. Our future work includes more complex modeling of cyber physical energy systems in Modelica by considering the hybrid simulation of continuous/discrete parts, developing a specified library of different types of attacks in Modelica for the cybersecurity community.

References

[1] S. Gorman, "Electricity grid in us penetrated by spies," *The Wall Street Journal*, vol. 8, 2009.

[2] J. Meserve, *Sources: Staged cyber attack reveals vulnerability in power grid*, CNN, 2007. [Online]. Available: http://www.cnn.com/2007//US/09/26/power.at.risk/index.html.

[3] R. Tan, H. H. Nguyen, E. Y. S. Foo, D. K. Y. Yau, Z. Kalbarczyk, R. K. Iyer, and H. B. Gooi, "Modeling and mitigating impact of false data injection attacks on automatic generation control," *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 7, pp. 1609–1624, Jul. 2017.

[4] P. M. Esfahani, M. Vrakopoulou, K. Margellos, J. Lygeros, and G. Andersson, "Cyber attack in a two-area power system: Impact identification using reachability," in *Proc. American Control Conf*, Jun. 2010, pp. 962–967.

[5] S. Sridhar and M. Govindarasu, "Model-based attack detection and mitigation for automatic generation control," *IEEE Transactions on Smart Grid*, vol. 5, no. 2, pp. 580–591, Mar. 2014.

[6] S. Sridhar and G. Manimaran, "Data integrity attacks and their impacts on scada control system," in *Proc. IEEE PES General Meeting*, Jul. 2010, pp. 1–6.

[7] T. Junjie, Z. Jianjun, D. Jianwan, C. Liping, X. Gang, G. Bin, and Y. Mengfei, "Cyber-physical systems modeling method based on modelica," in *Software Security and Reliability Companion (SERE-C), 2012 IEEE Sixth International Conference on*. IEEE, 2012, pp. 188–191.

[8] A. Teixeira, K. C. Sou, H. Sandberg, and K. H. Johansson, "Secure control systems: A quantitative risk management approach," *IEEE Control Systems*, vol. 35, no. 1, pp. 24–45, 2015.

[9] K. Pan, A. Teixeira, C. D. López, and P. Palensky, "Co-simulation for cyber security analysis: Data attacks against energy management system," in *Smart Grid Communications (SmartGridComm), 2017 IEEE International Conference on*. IEEE, 2017, pp. 253–258.

[10] L. Schenato, "To zero or to hold control inputs with lossy links?" *IEEE Transactions on Automatic Control*, vol. 54, no. 5, pp. 1093–1099, May 2009.

[11] K. Pan, A. Teixeira, M. Cvetkovic, and P. Palensky, "Cyber risk analysis of combined data attacks against power system state estimation," *IEEE Transactions on Smart Grid*, p. 1, 2018.

[12] G. Hug and J. A. Giampapa, "Vulnerability assessment of AC state estimation with respect to false data injection cyber-attacks," *IEEE Transactions on Smart Grid*, vol. 3, no. 3, pp. 1362–1370, Sep. 2012.

[13] P. Palensky, A. van der Meer, C. Lopez, A. Joseph, and K. Pan, "Applied cosimulation of intelligent power systems: Implementing hybrid simulators for complex power systems," *IEEE Industrial Electronics Magazine*, vol. 11, no. 2, pp. 6–21, Jun. 2017.

[14] D. Henriksson and H. Elmqvist, "Cyber-physical systems modeling and simulation with modelica," in *Proceedings of the 8th International Modelica Conference; March 20th-22nd; Technical Univeristy; Dresden; Germany*, no. 063. Linköping University Electronic Press, 2011, pp. 502–509.

[15] C. Chen, K. Zhang, K. Yuan, L. Zhu, and M. Qian, "Novel detection scheme design considering cyber attacks on load frequency control," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 5, pp. 1932–1941, 2018.

[16] M. Baudette, M. Castro, T. Rabuzin, J. Lavenius, T. Bogodorova, and L. Vanfretti, "OpenIPSL: Open-instance power system library — update 1.5 to "iTesla power systems library (iPSL): A modelica library for phasor time-domain simulations"," *SoftwareX*, vol. 7, pp. 34–36, jan 2018.

[17] V. Sanz, A. Urquía, F. E. Cellier, and S. Dormido, "System modeling using the parallel devs formalism and the modelica language," *Simulation Modelling Practice and Theory*, vol. 18, no. 7, pp. 998–1018, 2010.