INTELLIGENT ELECTRIC POWER GRIDS

SMART GRID CYBER SECURITY

Objectives

We will apply OpenModelica for cyber-attack impact evaluation. The IEEE 9-bus system is used as a case study. The objectives are

1. Learn the basics of risk management in smart grid cyber security.
2. Find signals susceptible to data integrity and/or data availability attacks.
3. Evaluate attack impact based on the OpenModelica tool for numerical simulations.

By performing attack impact evaluation through OpenModelica and analyzing the numerical outcomes (e.g., frequency deviations under different attack scenarios), this assignment will help you to consolidate the concepts learned during the lecture, with an emphasis on the objectives 1 and 2.

Methodology

You can find the following Modelica models in the model package "DelMod":

- "AutomaticGenerationControl" in the Control package. It is the model for the Automatic Generation Control (AGC) functionality. Users can specify the parameters of AGC. As talked in the lecture, AGC collects frequency deviations and tie-lines' power ow deviations and sends out mechanical power set-points to generators, through a Proportional-Integral (PI) control law.
- 'FalseDataInjection' in the AttackLibrary package. It is the model for False Data Injection (FDI) attack, a block which adds a step input to the existing measurement/control signals. Users can specify the time of the attack ('t1') and the attack intensity ('height').
- 'DataAvailabilityAttackTimed' in the AttackLibrary package. It is the model for a simple Denial-of-service (DoS) attack, a block which does not update the measurements/control signal for a user-defined time interval (from 't1' to 't2').
- 'DataAvailabilityAttackTriggered' in the AttackLibrary package. It is another model for a simple Denial-of-service (DoS) attack. This block will not update the measurements/control signal for a user-defined time interval (a period of 'dt') after 'trigger.start' was set to True.

You can also find the following given Modelica models to set up attack simulation scenarios:

- 'newGen' – The generator model for the IEEE 9-bus test system. It consists of a fourth order synchronous machine, along with automatic voltage regulator (AVR) and turbine governor model (GOV).
- 'NineBusForAGC' – The network model of the IEEE 9-bus test system. The generator model is from 'newGen'.
- 'NetworkAndAGC' – The aggregated model of the IEEE 9-bus test system equipped with AGC. Attack models can be also included.

Assignment

Task

The following steps shall be followed to evaluate the impact of pure FDI or DoS attacks against power system AGC:

Step 1: See the 9-bus system in Figure 1. This system is divided into three areas, each consisting of a generator and a load.

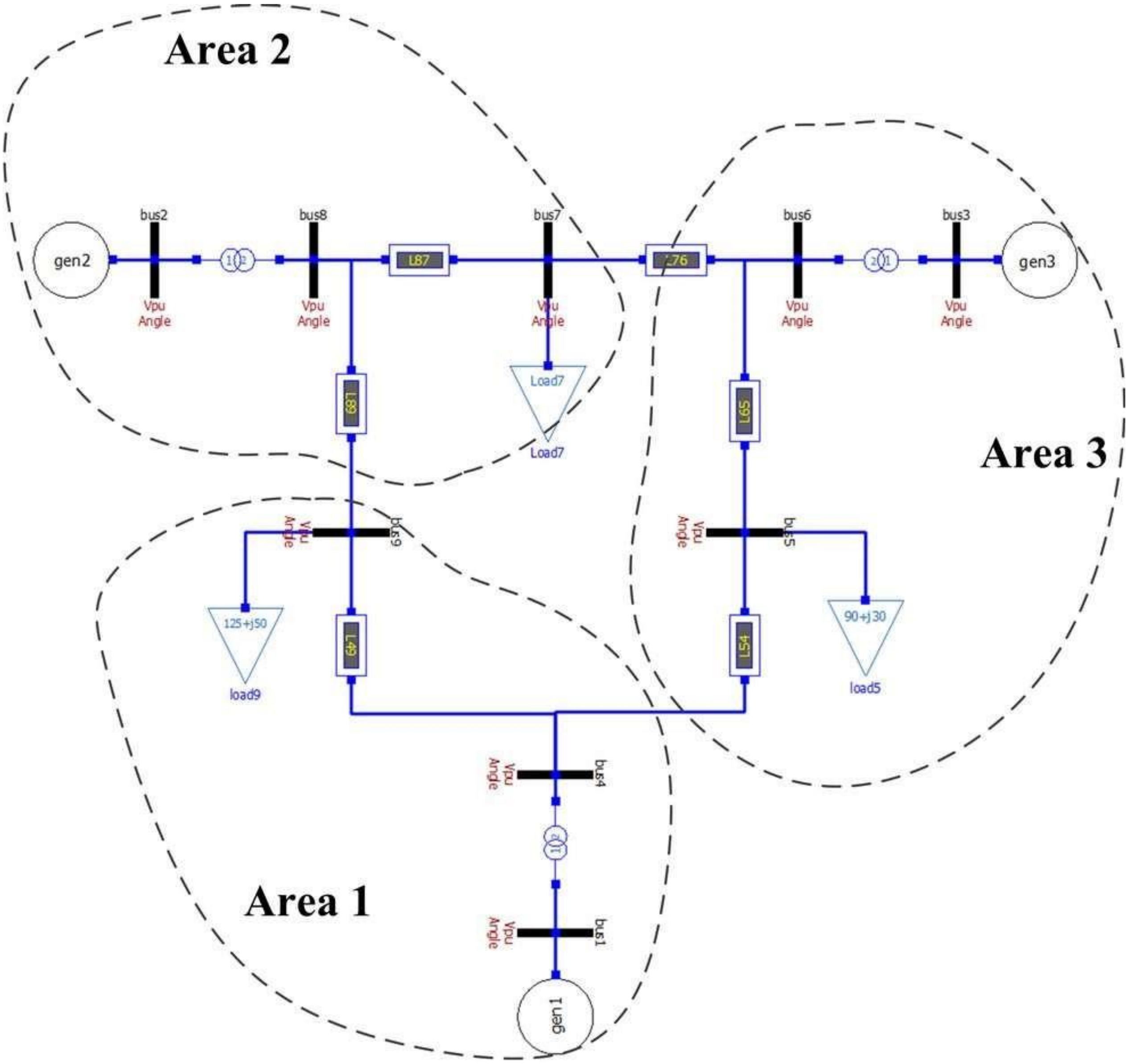

Figure 1: The 9-bus test system. It is divided into three areas, each consisting of a generator and a load.

Transmission lines (called tie lines) connect the areas. Each area has its own AGC controller to regulate the frequency of each area and the tie-line power flows. Use the given model in the packages 'NineBusForAGC' (similar to Figure 1) and 'AutomaticGenerationControl' (Figure 2) to build up the model for 9-bus system equipped with AGCs (for instance, one can build up an aggregated model like ‘NetworkAndAGC’ in Figure 3 but without the attack modules)

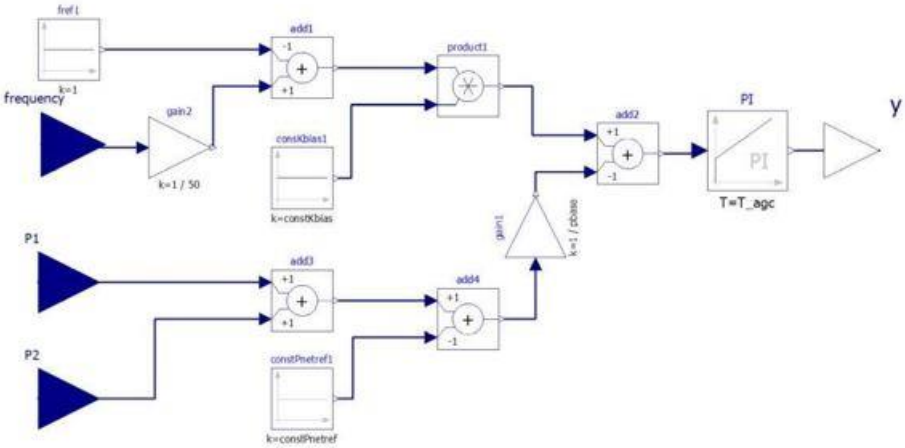

Figure 2: The AGC block.

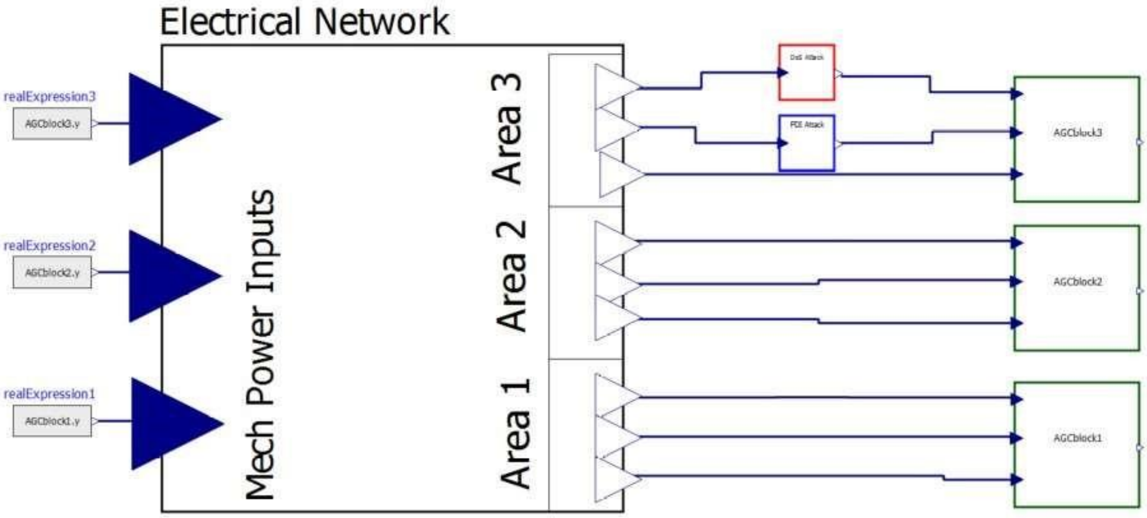

Figure 3: Complete network model with attack modules in OpenModelica.

Step 2: In the AGC modules we have provided the parameters of AGC for each area. Build a load event in one area (e.g., a step load change in Area 3 that the load is increased by 10%) and simulate in OpenModelica. See how a load change can cause frequency deviations and how AGC can restore the frequency to nominal values.

Step 3: Simulate different attack scenarios. Use the blocks of ‘FalseDataInjection’ and ‘DataAvailabilityAttackTimed’ to simulate attacks. The following attack scenarios should be considered:

1. FDI attacks on power flow measurement and AGC output signal of Area 3, individually. In this simulation case, the AGC control system is operating normally at the beginning. The total power generation and consumption are balanced (so there is NO step-load event). At time 100s, the FDI attack takes place. For attack on power flow measurement, the FDI would inject a positive value, while for attack on AGC output signal, the FDI would inject a negative value with the same magnitude.

2. DoS attacks on power flow measurement and AGC output signal of Area 3, individually. To see the impact, add a load step event (at time 100s in Area 2), and launch a DoS attack in Area 3. In both cases, the DoS attack occurs at 99s and stops at 120s.
3. Combined Attacks (there is NO load step event, we are now focusing on comparing combined attacks with pure FDI attacks in scenario 1):
    - a) An FDI attack corrupts the power flow measurement of Area 3 (just as in the first case). At the same time, a DoS attack is launched on the AGC output signal of Area 3 (from 99s to 120s).
    - b) The FDI attack still corrupts the power flow measurement of Area 3, but the DoS attack is now launched on the frequency measurement of Area 3 that it starts at 99s and stops at 120s.

Step 4: (Optional) Other attack scenarios can be also simulated.

Step 5: Export the figures of the aggregated models like Figure 3 under each attack scenario. Plot the figures of simulations results on frequency deviations of all three areas, under each attack scenario.