**SIMBA Simulation Configuration File High Level Specification**

The SIMBA Input configuration file provides five distinct types of information:

1. Simulation configuration parameters
   * A variety of values that define the start and end times for the requested simulation and specification of the GridLab-D model that will be used.
2. Message Creation Thresholds:
   * Vmin, Vmax, Pmin, Pmax – These values are used by Output\_Message\_Creation() to determine if/when individual AMI meters should generate ODEventNotification (alarm) messages (Message Type B).
3. Message Creation, Send, and Receive Probabilities:
   * A: PMeterValue-Request PMeterValue-Respond – These probabilities determine whether correct Request and Respond messages are generated at each appropriate timestep (15 minutes) for meter values. (Output\_Message\_Creation() will generate message reading request and response messages with these probabilities. Meters may send values even when a request message is not generated (corresponding to messages that we fail to capture) [Default Values: 1]
   * B: PMeterEventSend – This probability is used by Output\_Message\_Creation() to determine whether a correct ODEventNotification message is sent by a meter when one of the message creation thresholds is triggered. [Default Value: 1]
   * C: PMeterDisconnect-Trigger PMeterDisconnect-Request PMeterDisconnect-Action: These probabilities are used by Input\_Message\_Creation() to determine whether a Meter Disconnect action is requested by the control center at each timestep (this is implemented periodically on a coarse time step, say every 5 minutes), whether a meter disconnect message is generated, and whether the requested meter actually disconnects. (Note: The Meter Disconnect Trigger is evaluated first. If/when the Meter Disconnect Trigger is activated, then the other two probabilities are used to determine whether a message is generated and whether the meter disconnects. The meter may disconnect even if no meter disconnect message is generated (indicating that we missed the message in our capture device). [Default Values: 0]
   * D: PDNP3Value-Request PDNP3Value-Response -These probabilities determine whether correct Request and Respond messages are generated at each appropriate timestep (4 seconds) for substation values. (Output\_Message\_Creation() will generate message reading request and response messages with these probabilities [ Default Values: 1]
   * E: PVoltageControl-Send PVoltageControl-Action– The timestamp for all voltage control messages is pre-specified below. These probabilities are used to determine whether a message requesting the voltage control action is sent and whether the voltage control action is implemented. (The action can be taken even if the message is not generated and vice versa (corresponding to messages that we fail to capture.) [Default Values: 1]
   * F: PSwitchControl-Send PSwitchControl-Action– The timestamp for all switch control (reconfiguration) messages is pre-specified below. These probabilities are used to determine whether a message requesting a switch status change is sent and whether the switch control action is implemented. (The action can be taken even if the message is not generated and vice versa (corresponding to messages that we fail to capture.) [Default Values: 1]
4. Pre-Specified Event Messages (Input\_Message\_Creation() is responsible for inserting each of the actions below into the GridLab-D model and generating the appropriate messages (subject to the probabilities specified above).
   * VoltageControlActions: A list of voltage control actions (LTC tap changes or capacitor bank status changes) will be specified in the configuration file. Each item in the list will include a timestamp , a device identifier, and a setpoint.
     + Note: Generally the voltage control actions should only be specified during low or high voltage conditions in the network. Therefore, it may be necessary to first run GridLab-D without any voltage control actions. The results from that first run can then be used to (manually) generate a list of voltage control actions to include in the simulation
   * SwitchStatusActions: A list of switch status changes will be specified in the configuration file. Each item in the list will include a timestamp, a device identifier, and the action (OPEN/CLOSE). Needs to be some kind of source transfer situation.
   * Meter connect/disconnect events. There's no realistic scenario we're worried about. We're just trying to generate some meters going on and off.
5. Attacks

For the November 2017 exercise 5 types of attacks are considered to be in scope:

* + AMI.1: *Authorized Employee Issues Unauthorized Mass Remote Disconnect*
    - For this attack type, a list of meters and timestamps will be provided. At the given timestamps Input\_Message\_Creation() will trigger meter disconnects for all meters on the list. (Note: The creation of these messages and the likelihood of the disconnect will be subject to the PMeterDisconnect-Request PMeterDisconnect-Action probabilities only.)
  + AMI.8: *False Meter Alarms Overwhelm AMI and Mask Real Alarms*
    - For this attack type, a list of meters and timestamp will be provided. At the given timestamp Input\_Message\_Creation() will create ODEventNotification (alarm) messages for all specified meters.
  + DGM.6: *Spoofed Substation Field Devices Influence Automated Responses*
    - For this attack type, Output\_Message\_Creation() will artificially modify the connectivity, power or voltage status/readings at specified devices. A list of spoofed devices will be provided for this attack. Each item in the list will include a start and end timestamps, a device identifier, a quantity identifier (connection status, power, voltage), and a code indicating the change that should be calculated. (The “codes” will indicate whether a value should be reduced to 0, multiplied by a factor, set to a specific value, etc. [The ”codes” are to be determined.] Note: The creation of these spoofed messages does not change anything about how the GridLab-D simulation is run.
  + DGM.10: *Switched Capacitor Banks are Manipulated to Degrade Power Quality*
    - For this attack type, a list of substation devices and timestamps will be provided. At the given timestamp Input\_Message\_Creation() will trigger substation voltage or switch control messages for specified device(s). (Note: The creation of these messages and the likelihood of their implementation will be subject to the PVoltageControl-Send PVoltageControl-Action and PSwitchControl-Send PSwitchControl-Action probabilities.)
  + Denial of Service Attack:
    - For this attack type, a list of devices with start and end timestamps will be provided. Between the start and end timestamps all messages from the specified devices will not be created.

Note: For now, all attacks can be manually specified in the configuration file. Eventually, we may want to write code to build attacks automatically based on a small number of input parameters (e.g. attack type, attack duration, # of devices impacted, etc.)