

One Command to Force Widespread Under- Frequency Load Shedding



Control Systems: Evaluating the Risk

Workshop 2008

Albuquerque, New Mexico

June 24, 2008

Scenario Disclaimer

- **The following scenario is fictional and has been created for the purpose of:**
 - Providing a “backdrop” to exercise Sandia’s threat-to-consequence risk analysis framework and tools being developed under the DOE/OE National SCADA Test Bed Program; and
 - To provide a baseline to demonstrate the need to identify and characterize potential exploits that can provide high-consequence impacts to critical infrastructures.

Scenario Assumptions

- By tripping generator breakers, it may be possible to cause a wide-spread under-frequency load shedding
- This can only be accomplished if the system is in stage 2 alert

What are some of the constraints?

- Information needs?
 - Confirm that the selected generators are on line
 - Know the console ID, substation ID and breaker IDs for each select generators
 - Know when to trigger the event
- Must compromise selected organizations to load and set the operating parameters of the rogue software?
- Must have the means and resolve to prepare and validate the rogue software?
- If any one of these constraints are not met, the scenario can not be achieved

Need a development lab?

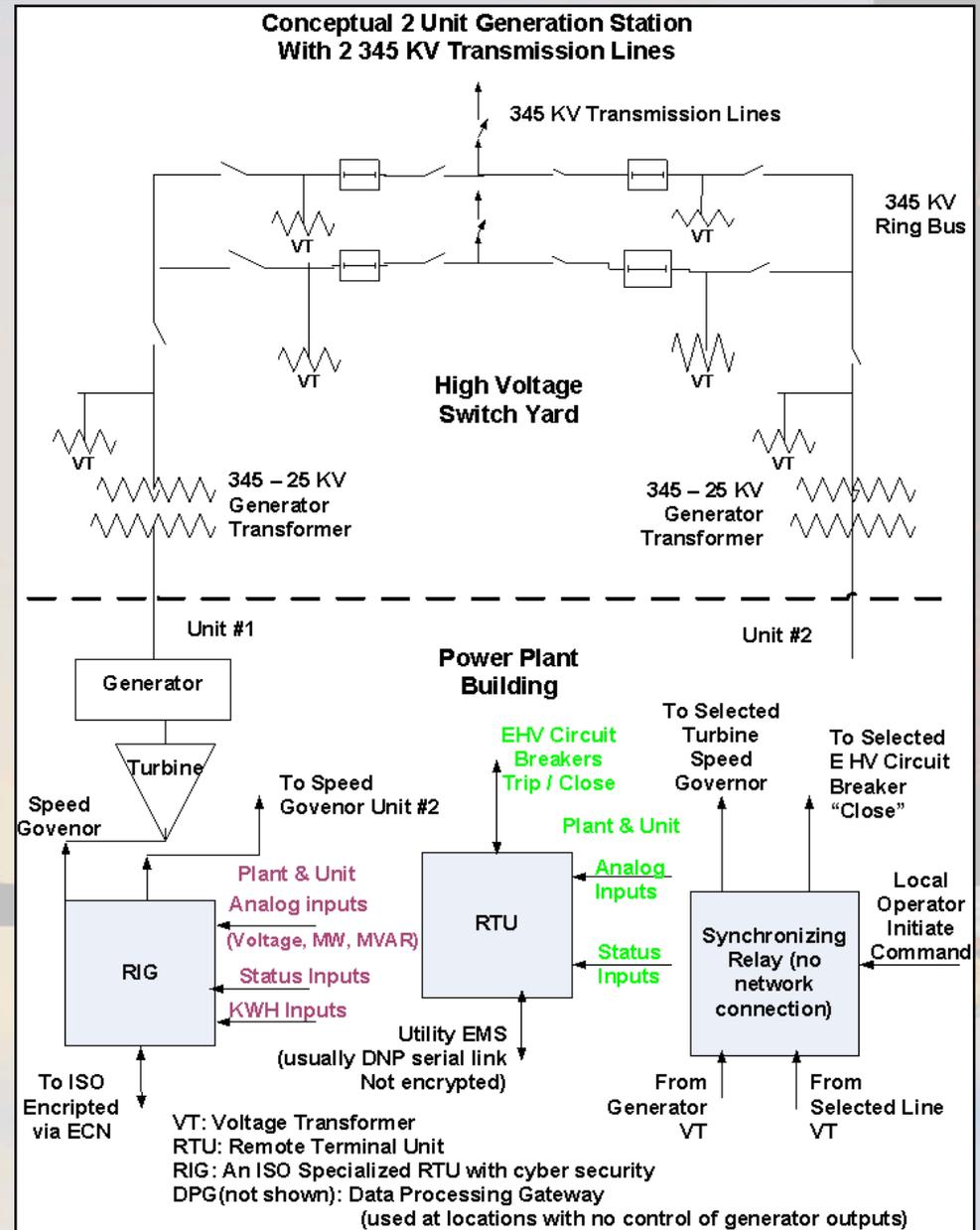


Scenario Objectives

- Overall objective
 - Minimize adversary exposure
 - Execute attack on date/time or by command
- Results objective
 - Trip enough generators to cause under-frequency load shedding
 - Time synchronize breaker trips
 - Select generators to provide sufficient timing margin of error
 - Assume Stage 2 alert

Consider Potential Attack Points

- Two breakers per generator via the RTUs must be tripped.
- Entry Point Options:
 - Communications between EMS and RTU
 - Planting surrogate software in EMS/SCADA masters
 - Planting surrogate software in RTU
 - Planting surrogate software in Front End Processors (FEP)



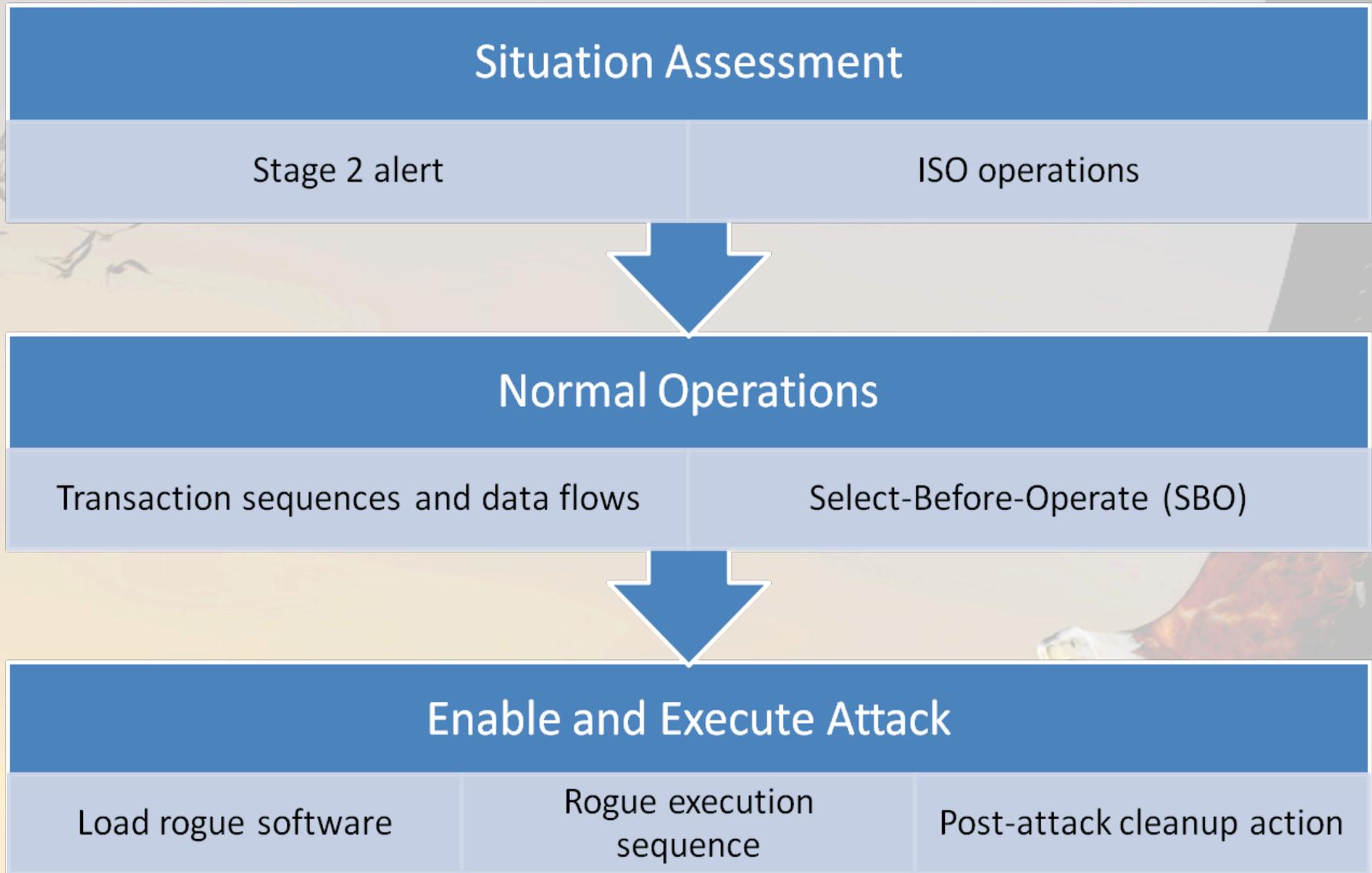
FEP Point-of-Entry

- FEPs:
 - Require no human intervention
 - Are an interface between the EMS/SCADA master and the RTU communication lines
 - Contain the points-list that associate breaker IDs with RTU addresses
 - If enabled, performs security functions
 - Encryption/decryption authentication/authorization before messages are sent to the RTU

Simply Protocol Sniffing is Not Enough

- Not credible to simply listen to traffic between EMS/SCADA and RTUs
 - Breaker points are rarely operated
- Knowledge of how FEPs operate are needed

Scenario Progression



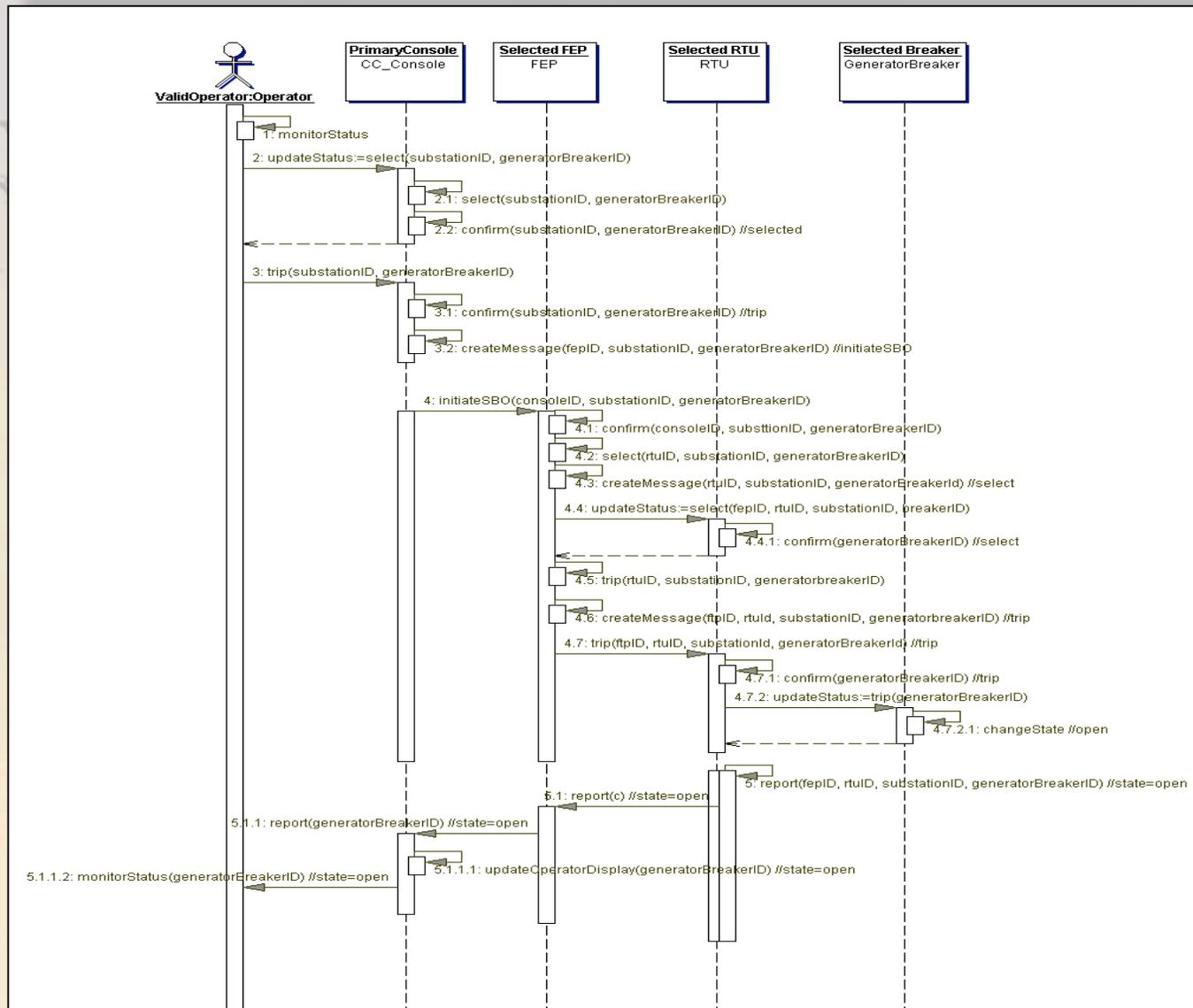
Rogue Software

- When to load?
 - At the manufacturer
 - Packaged with a new FEP software release
- What will it do?
 - Will generate/send breaker trip commands;
 - Until repeat-timing parameter expires; and
 - May remain resident on the FEP

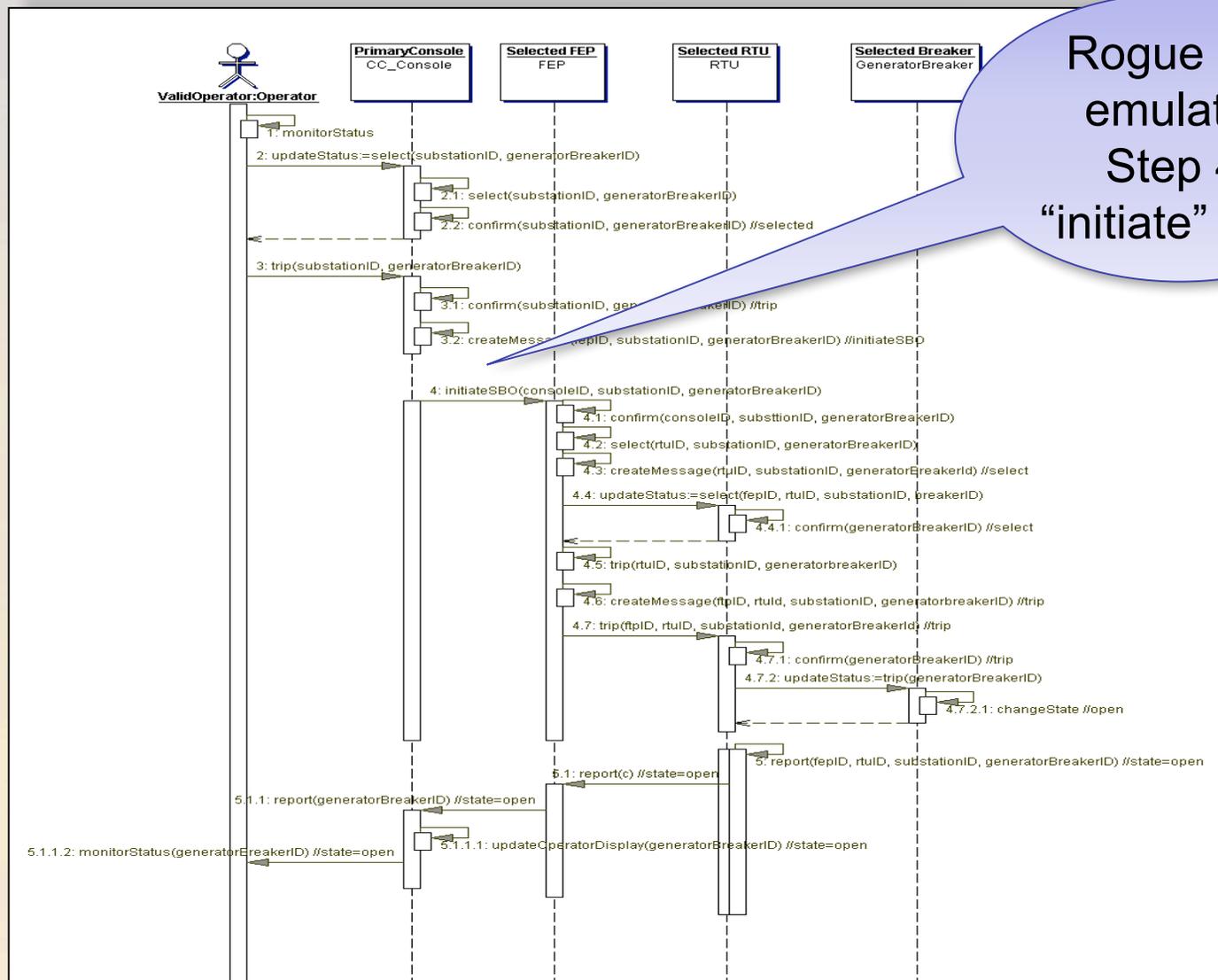
Execution Time

- Rogue software is installed when the new FEP software is brought on-line
 - Timing parameters are pre-set in rogue software
- Pre-timing selection was based on information:
 - On the web site
 - Monitor the total ISO system load
 - When Stage 2 alerts are typically reported

Typical Select Before Operate (SBO) Transaction



Modified SBO Transaction



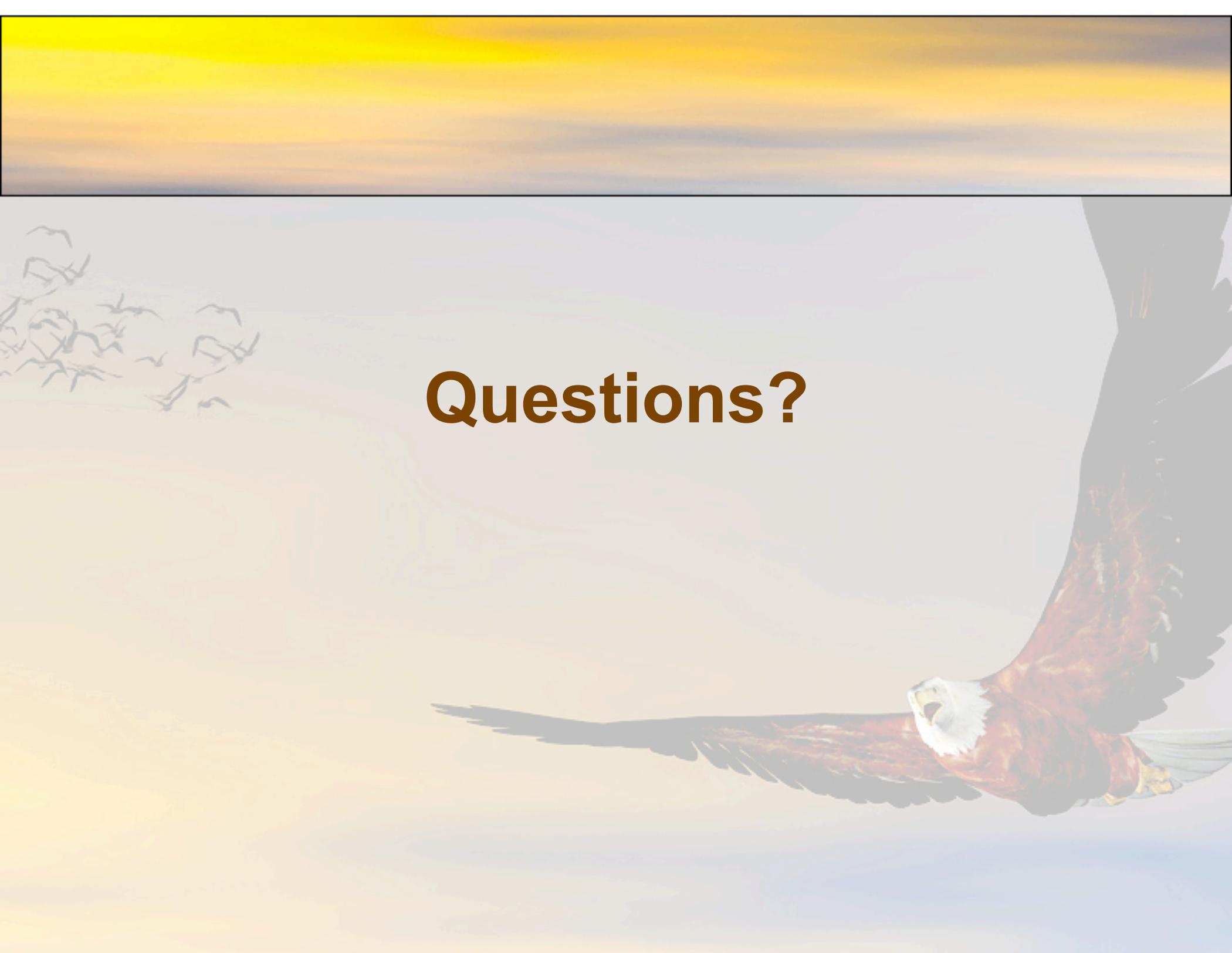
Rogue SW emulates Step 4: "initiate" SBO

Progression

- Step 4 (previous slide) requires the rogue software to know:
 - consoleID
 - substationID
 - generatorBreakerID (both breaker IDs – two messages)
- Upon receipt of the initiateSBO messages
 - FEP software performs Step 4.1
 - Which then triggers steps 4.2 through 4.7
- Rogue software monitors the messages from the RTU to the FEP
 - Verify SBO function is executed correctly
 - If so, the breakers have been opened
 - If not, it repeats the command

In Summary

- Rogue code is planted in the FEP software
- Initiation requires only one command per FEP
 - initiateSBO(consoleID, substationID, generatorBreakerID)
 - FEP software generates select and trip (operate) messages
 - RTUs confirm/acknowledge select and trip commands, and send trip message to selected generator breakers
 - Generator breakers open breaker & report change of state to RTU
 - RTU reports breaker “state=open” to FEP
 - FEP reports breaker “state=open” to control center console
 - Control center console updates operator display

A bald eagle is shown in flight, its wings spread wide, flying from the right side of the frame towards the left. The eagle has a white head and neck, and dark brown feathers on its wings and body. The background is a soft, hazy sunset sky with warm yellow and orange tones. In the upper left corner, a large flock of birds is seen flying in the distance. The overall scene is serene and majestic.

Questions?