Transmission

Tim Yardley – University of Illinois
Information Trust Institute

NITRD TTS Workshop

July 18-20, 2011

Setting The Stage

- Fairly static security settings
  - Tailored to their mission
  - Predominately perimeter security
- Generally single operating domain
- Varied technology and communication mediums in use
- Some stringent requirements (“low” msec)
- Some very loose requirements (hourly, daily)
- Humans and Machines involved

Use Case 1

Use case 1

- Real-Time Normal Transmission Operations Using Energy Management System (EMS) Applications and SCADA Data
  - NISTIR-7628, pg. 129

- “Normal” Operations
  - Things are generally operating per-norm

Use case 1 - Description

- Transmission operations involve monitoring and controlling the transmission system using the SCADA system to monitor and control equipment in transmission substations. The EMS assesses the state of the transmission system using applications typically based on transmission power flow models. The SCADA/EMS is located in the utility's control center, while the key equipment is located in the transmission substations. Protective relaying equipment monitors the health of the transmission system and takes corrective action within a few milliseconds, such as tripping circuit breakers if power system anomalies are detected.

Use case 1 - Scenario

- Transmission normal real-time operations involve monitoring and controlling the transmission system using the SCADA and EMS. The types of information exchanged include
  - Monitored equipment states (open/close), alarms (overheat, overload, battery level, capacity), and measurements (current, voltage, frequency, energy)
  - Operator command and control actions, such as supervisory control of switching operations, setup/options of EMS functions, and preparation for storm conditions
  - Closed-loop actions, such as protective relaying tripping circuit breakers upon power system anomalies
  - Automation system controls voltage, VAR, and power flow based on algorithms, real-time data, and network linked capacitive and reactive components

Use case 1 – SG Characteristics

- Characteristics
  - Provides power quality
  - Optimizes asset utilization
  - Anticipates and responds to system disturbances
- Potential Stakeholder issues
  - Customer safety
  - Customer device standards
  - Demand response acceptance by customers

Use case 1 – Cyber Security

- Integrity is vital to the safety and reliability of the transmission system
- Availability is critical to protective relaying (e.g. < 4 ms) and operator commands (e.g., 1 s)
- Confidentiality is not important

Use case 1 – Potential Actors

- Operators
- Field Technicians
- Control Centers
- Substations
- Devices, Power Assets
- Vendors, Third party contractors
- Attackers
- External Actors
  - Any of the above, but not in your control

Use case 1 – Potential Transactions

- Monitoring
  - Loss of, Inaccurate, Verifiable
- Maintenance operations
  - Pre, On-going, Post
- Automation
  - External, Internal, Cooperative
- System experiences a disturbance
  - Physical, Cyber, or Cyber-Physical

Use case 1 – Potential Information

- Topology
- Planning data
  - Models, Forecasts, etc.
- Operational data
  - Measurements, Alarms, etc.
- Out-of-band communication
  - Field interactions, External interactions, etc.
- Ancillary information
  - Weather, News reports, etc.

Use case 1 – Example

- Poll substation for data
- Input data into EMS/state estimation
- Output current state into
  - Contingency analysis
  - Control actions
  - Etc.
- Analyze/Apply results

Use Case 2

Use case 2

- Real-Time Emergency Transmission Operations
  - NISTIR-7628, pg. 131
- “Emergency” Operations
  - Something bad has happened

Use case 2 - Description

- Transmission operations involve monitoring and controlling the transmission system using the SCADA system to monitor and control equipment in transmission substations. The EMS assesses the state of the transmission system using applications typically based on transmission power flow models. The SCADA/EMS is located in the utility's control center, while the key equipment is located in the transmission substations. Protective relaying equipment monitors the health of the transmission system and takes corrective action within a few milliseconds, such as tripping circuit breakers if power system anomalies are detected.

Use case 2 - Scenario

- During emergencies, the power system takes some automated actions and the operators can also take actions
  - Power System Protection: Emergency operations handles under-frequency load/generation shedding, under-voltage load shedding, load tap changer (LTC) control/blocking, shunt control, series compensation control, system separation detection, and wide area real-time instability recovery
  - Operators manage emergency alarms
  - SCADA system responds to emergencies by running key applications such as disturbance monitoring analysis (including fault location), dynamic limit calculations for transformers and breakers based on real-time data from equipment monitors, and pre-arming of fast acting emergency automation
- SCADA/EMS generates signals for emergency support by distribution utilities (according to the T&D contracts)
  - Operators performs system restorations based on system restoration plans prepared (authorized) by operation management

Use case 2 – SG Characteristics

- Characteristics
  - Provides power quality
  - Optimizes asset utilization
  - Anticipates and responds to system disturbances
- Potential Stakeholder issues
  - Customer safety
  - Customer device standards
  - Demand response acceptance by customers

Use case 2 – Cyber Security

- Integrity is vital to the safety and reliability of the transmission system
- Availability is critical to protective relaying (e.g. < 4 ms) and operator commands (e.g., 1 s)
- Confidentiality is not important

Use case 2 – Potential Actors

- Operator
- Field Technician
- Control Center
- Substation
- Device
- Emergency Agency or Person
- External Actor
  - Any of the above, but not in your control

Use case 2 – Potential Transactions

- Communication
  - None, Physical only, Full
- Islanding
  - Controlled, Forced,
- Alarming
  - Verifiable, False
- Analysis
  - Locatable, No Results
- Restoration
  - Internal, External, Cooperative

Use case 2 – Potential Information

- Topology
- Planning data
  - Models, Forecasts, etc.
- Operational data
  - Measurements, Alarms, etc.
- Out-of-band communication
  - Field interactions, External interactions, etc.
- Ancillary information
  - Weather, News reports, etc.

Use case 2 – Example

- Prioritize alerts and alarms
- Poll substations for data (priority based)
- Input data into EMS/state estimation
- Output current state into
  - Contingency analysis
  - Control actions
    - Enable disturbance monitoring
    - Enable emergency automation
  - Etc.
- Analyze/Apply results

Scenarios

Scenario 1

- Areas that are operating close to margins determined by contingency analysis or state estimation may be of more concern in the short time frame than others. This means that areas that are near capacity, under maintenance, experiencing issues, or more “fragile” than others may have dynamic constraints that change with conditions. Further, these locations will vary based on state estimation solutions, contingency analysis, etc.

Scenario 2

- Some areas are more critical than other areas due to how they are connected, how the BES is constructed, or the current state of the system. For example, lines that are inter-ties, or connected to major assets feeding high demand areas may be more important than others despite their relatively lower capacity. Another example may be that a location is geographically distant from generation and as a result has voltage stability issues due to this topology.

Tailoring

Properties

- Availability, Authentication, Integrity, Timeliness, Non-repudiation, logging, time accuracy, alarm reporting, provenance, guaranteed latency, Privacy, Confidentiality

Tailoring Cases

- State Estimation
  - Operational vs Pricing/Market
- Confidentiality
  - It actually is important… Emergency operations
  - Perhaps Authentication can handle this?

Property Working Document

- Automated machine to machine actions for distributed protection and control
  - Less impt: Privacy, Confidentiality
  - SCADA - slow
  - Line protection – fast
- Authentication
  - Emergency response (drop auth if necessary?)