Design Tradeoffs and Cyber Security for Microgrids

Jason Stamp, Ph.D.
Sandia National Laboratories
10 August 2016
**Example Microgrid Load Categorization/CONOPS**

- **Loads/buildings:**
  - Tier C – critical to the site; usually have dedicated backup generators. Tier C\(_i\) are non-interruptible and will include UPS, while Tier C\(_u\) can endure short losses of electrical power.
  - Tier P – nice to have, but that can be switched on or off discretionally. Some may have generators. May be designated ahead of time, or promoted ad hoc (depending on their configuration).
  - Tier O – not be powered on microgrid operations.
  - Tier O\(_P\) – too small to merit the cost of automation (e.g. street or parking lights).

- **“Seamless”:**
  - Planned
  - Unplanned

---

**Fig. 1. Basic ESM CONOPS (solid lines indicated energized equipment, and dashed are de-energized)**

- (a) All buildings on the microgrid are powered by the local utility; DGs are off and RE is outputting energy (C, P, and O correspond to load tiers)
- (b) Immediately after the loss of utility power, no loads or generation are active (distributed UPSs support Tier C/U load)
- (c) DGs power up and first energize the buildings they are designated to support; this is exactly the same as non-microgrid backup operation
- (d) The PCC opens and MV switching disconnects all loads and RE from the microgrid; one-by-one, DERs synchronize to energize the microgrid
- (e) All Tier C loads are powered, and after a delay RE sources and priority loads return to service (this is the stable ESM operational state)
- (f) Once utility power returns, the PCC reconnects the microgrid in a careful and coordination fashion
- (g) After reconnection, DGs shut down (active loads are not affected as they are being supplied by the utility)
- (h) The microgrid ESM restores the site MV network to its normal state, which allows Tier O loads to be served
## Taxonomy of Quantitative Metrics for Design

<table>
<thead>
<tr>
<th>Benefit</th>
<th>Operating Mode</th>
<th>Abbreviation</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Normal</td>
<td>N</td>
</tr>
<tr>
<td>Technical</td>
<td>Typical Emergency</td>
<td>TE-TC</td>
</tr>
<tr>
<td>Financial</td>
<td>Abnormal Emergency</td>
<td>AE-TC</td>
</tr>
<tr>
<td>Environmental</td>
<td></td>
<td>N-EN</td>
</tr>
<tr>
<td></td>
<td></td>
<td>TE-EN</td>
</tr>
<tr>
<td></td>
<td></td>
<td>AE-EN</td>
</tr>
</tbody>
</table>

### Examples:
- Normal, technical (N-TC): Improved power quality if equipment from resiliency measures support it
- Normal, technical (N-TC): Simpler backup testing through improved control and energy flexibility
- Normal, financial (N-FN): Reducing energy billing costs through energy consumption management
- Normal, financial (N-FN): Revenue from market/demand response participation or from energy contracts with utilities
- Normal, environmental (N-EN): Deferred emissions from reduced consumption or improvements to utility operations
- Typical emergency, technical (TE-TC): Improved reliability for critical loads: systems designed for resiliency could be used to support critical load during normal outages if there are failures in normal backup procedures or equipment
Microgrid Resiliency Advanced Metrics

- Expected performance metrics can be measured as statistics
- Example:
  - Analysis for 1/3/5/28 day outages, histogram shows time Cu load is unserved, given that it happens
  - Base case/MG1/MG2: 5%/0.4%/0.1% rate of critical/uninterruptible load unserved per outage
- Which histogram shows best cost/benefit?
  - Metrics can use expected value only, or...
  - A combination of expected value, variance, and/or frequency of extremes

Balancing Financial and Resilience Metrics

$z = x + y$

NPV of total microgrid investment ($z$)

$\text{Net investment in resiliency (y)}$

NPV of total cost savings and revenue from grid-connected operations ($x$)
The Microgrid Design Toolkit (MDT) is a decision support software tool for microgrid designers in the early stages of the design process.

The software employs powerful search algorithms to identify and characterize the trade space of alternative design decisions in terms of user defined objectives. Common examples of such objectives are cost, performance, and reliability.

Once the trade space has been characterized, the software provides many views and features to help explore that trade space to extract information.
Microgrid Design Toolkit (MDT)

- MDT 1.0 Beta is now available for download
  - Has been downloaded more than 117 times since posting on 4/6/16.

- Software is being reviewed by an external advisory board

- Past usage:
  - The US Marine Corps Expeditionary Energy Office (E2O) used the MDT to assess microgrid power systems and Mobile Electric Hybrid Power Sources (MEHPS) for expeditionary units and brigades.
  - The SPIDERS Program used a predecessor to the MDT to develop the preliminary microgrid designs for 3 military bases.
  - The City of Hoboken, NJ used a predecessor to the MDT to develop the preliminary microgrid design for backup power in response to Hurricane Sandy.

- Current uses of the MDT include:
  - Continued use for the Marine Corps
  - A backup power system/microgrid design study for the UPS Worldport facility in Louisville, KY.
  - A backup power system/microgrid design study for the city of New Orleans, LA.
Sandia’s Control System Security Research

Provide decision makers with actionable information

- Red Team Assessments
- Field Device Analysis
  - PLC monitoring and forensics
  - PLC firmware forensics
  - ICS network detection for ICS traffic
- Emulytics (SCEPTRE)
- Exercise/Test Bed support

Design resilient systems to withstand cyber-attacks

- Research next generation security solutions
- Partner with industry to “push” solutions to market

Mission: To reduce the risk of critical infrastructure disruptions due to cyber attacks on control systems.
Control System Architecture

User Interfaces
- Human-Machine Interface (HMI) software
- Status displays
- Switches and dials

Control System Apps
- Supervisory Control and Data Acquisition (SCADA)
- Distributed Control Systems (EMS/DCS)
- Data Historians

Field Devices
- Programmable Logic Controllers (PLC)
- Remote Telemetry Units (RTU)
- Intelligent Electronic Devices

Sensors
- Thermocouples
- Accelerometers
- Photoresistors

Actuators
- Breakers/Switches
- Motors
- Valves

Physical Process
- Oil & Gas Refining
- Electrical Distribution and Transmission
- Manufacturing
Representative ICS Testing Environments

Emulytics™/SCEPTRE

Energy Exchange: Federal Sustainability for the Next Decade
SCEPTRE Operational Overview

- SCEPTRE provides a cyber-physical environment to show interaction between cyber-initiated events and the physical world
- Balances need for M&S accuracy against testing resources
  - Live system testing: potential damage to the real system and dangers to human life
  - Test bed systems: Expensive to build, maintain, configure, and operate
  - Labscale hardware testing setups: May require the context of a larger, networked system
- Devices (simulated, emulated, real) communicate/interact via ICS protocols
- All ICS devices are able to interact with the process simulation, providing both updates and subscribing to the current state of the simulation
- Overall simulation is able to bridge multiple infrastructures into the same experiment to show interdependencies
- Use cases:
  - Test and evaluation
  - Mission rehearsal
  - Other analysis: understand vulnerabilities and exploitable avenues, identify critical components on the control network, model infrastructure interdependencies, etc.
Cyber Security Architecture

- Microgrid cyber security reference architecture
- In addition to DoD IA controls, additional rigor will be applied to protecting data-in-motion and data-at-rest, along with ensuring such additional rigor does not impede the operational data exchange requirements of the SPIDERS microgrid
- Defense-in-depth using:
  - Enclaves
  - Functional Domains
Cyber Security Data Exchange

- **Process:**
  - Designate actors
  - Describe data flows using tables
  - Assign enclaves
  - Develop functional domains
  - Design cyber security controls

### Example Flat Control System

![Example Flat Control System Diagram]

#### Data Exchange Table Format

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
<th>Example Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Exchange</td>
<td>Type: Type of data exchange to occur</td>
<td>monitor, control, report, write</td>
</tr>
<tr>
<td></td>
<td>Interval: How often data exchange occurs</td>
<td>e.g. milliseconds, seconds</td>
</tr>
<tr>
<td></td>
<td>Method: How data will be exchanged</td>
<td>unicast, multicast, broadcast</td>
</tr>
<tr>
<td></td>
<td>Latency Tolerance: Relative importance of exchanging the data</td>
<td>high, medium, low</td>
</tr>
<tr>
<td></td>
<td>Latency Tolerance: Tolerance to delayed control or delayed data exchange</td>
<td>high (delays do not affect operation), medium, low</td>
</tr>
</tbody>
</table>

| Data        | Type: Type of data to be exchanged                                           | voltage, setpoint, status           |
|             | Accuracy: Necessary precision/timeliness of data                             | significant digits, time units      |
|             | Volume: Amount of data transferred per exchange                              | e.g. bytes, kilobytes, etc.         |
|             | Reliability: Necessity of access to control processes and data               | critical, important, informative    |

| Information Assurance | Confidentiality: Importance of preserving restrictions to control processes and information access (based on risk to system operations and/or system security) | high, medium, low                  |
| Information Assurance | Integrity: Importance of preventing unauthorized changes to control processes or data, including authenticity (based on reliability with respect to operations) | high, medium, low                  |
| Information Assurance | Availability: Importance of timely and reliable access to control processes and data (based on priority and latency tolerance with respect to operations) | high, medium, low                  |

### Data Exchange Attributes for Automated Grid Management and Control (AGMC) Operations

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>FEP</th>
<th>FEP</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Generator controller</td>
<td>Generator controller</td>
</tr>
<tr>
<td>Exchange</td>
<td>Type</td>
<td>monitor</td>
<td>control</td>
</tr>
<tr>
<td></td>
<td>Interval</td>
<td>seconds</td>
<td>seconds or minutes</td>
</tr>
<tr>
<td></td>
<td>Method</td>
<td>unicast</td>
<td>unicast</td>
</tr>
<tr>
<td></td>
<td>Priority</td>
<td>medium</td>
<td>medium</td>
</tr>
<tr>
<td></td>
<td>Tolerance</td>
<td>medium</td>
<td>low</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Data</th>
<th>Type</th>
<th>run/start/ATS status, fuel level, active &amp; reactive output, frequency</th>
<th>start/stop/mode/breaker control, voltage settings, governor droop settings</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Accuracy</td>
<td>1 decimal, second</td>
<td>1 decimal, second</td>
</tr>
<tr>
<td></td>
<td>Volume</td>
<td>bytes</td>
<td>bytes</td>
</tr>
<tr>
<td></td>
<td>Reliability</td>
<td>important</td>
<td>critical</td>
</tr>
</tbody>
</table>

**Information Assurance**

| Confidentiality | medium | medium |
| Integrity      | medium | high   |
| Availability   | high   | high   |
Defense-in-depth: Application of Enclaves and Functional Domains
Cyber Security Quantitative Analysis

H/M/L Sensitivity Scores for Functional Domains

<table>
<thead>
<tr>
<th>Functional Domain</th>
<th>Read/Write</th>
<th>Confidentiality</th>
<th>Integrity</th>
<th>Availability</th>
<th>Subtotal</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>HMI-Server</td>
<td>Read</td>
<td>2</td>
<td>3</td>
<td>2</td>
<td>7</td>
<td>13</td>
</tr>
<tr>
<td></td>
<td>Write</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>6</td>
<td>13</td>
</tr>
<tr>
<td>Server-FEP</td>
<td>Read</td>
<td>2</td>
<td>3</td>
<td>2</td>
<td>7</td>
<td>13</td>
</tr>
<tr>
<td></td>
<td>Write</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>6</td>
<td>13</td>
</tr>
<tr>
<td>FEP-RTU</td>
<td>Read</td>
<td>1</td>
<td>3</td>
<td>3</td>
<td>7</td>
<td>15</td>
</tr>
<tr>
<td></td>
<td>Write</td>
<td>2</td>
<td>3</td>
<td>3</td>
<td>8</td>
<td></td>
</tr>
<tr>
<td><strong>Totals</strong></td>
<td>Both</td>
<td>11</td>
<td>16</td>
<td>14</td>
<td>41</td>
<td>41</td>
</tr>
</tbody>
</table>

Red Team Scoring Results

<table>
<thead>
<tr>
<th>Architecture</th>
<th>Access</th>
<th>Compliance</th>
<th>Confidentiality</th>
<th>Integrity</th>
<th>Availability</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Flat</td>
<td>High</td>
<td>Insecure</td>
<td>0</td>
<td>0</td>
<td>8</td>
<td>8</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Hardened</td>
<td>9</td>
<td>0</td>
<td>14</td>
<td>23</td>
</tr>
<tr>
<td></td>
<td>Enclaved</td>
<td>High</td>
<td>Insecure</td>
<td>0</td>
<td>0</td>
<td>8</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Hardened</td>
<td>9</td>
<td>0</td>
<td>14</td>
<td>23</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Medium</td>
<td>Insecure</td>
<td>7</td>
<td>6</td>
<td>11</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Hardened</td>
<td>9</td>
<td>6</td>
<td>14</td>
<td>29</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Low</td>
<td>Insecure</td>
<td>11</td>
<td>6</td>
<td>16</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Hardened</td>
<td>11</td>
<td>6</td>
<td>16</td>
<td>33</td>
</tr>
<tr>
<td><strong>Maximum Possible Score</strong></td>
<td>11</td>
<td>16</td>
<td>14</td>
<td>41</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Advanced Field Device Monitoring

PLCs are vulnerable to targeted attacks that cost millions in equipment damage, lost operation, or injured personnel.

A backplane analysis system examines the communication between PLC modules.

PLCs are not monitored for security compromise.

Cyber attacks on the control systems will result in anomalies visible on the PLC backplane.

It is not enough to build “secure” products. The ability to inspect and detect is necessary for systems that will be in place for decades.

New Capabilities for PLCs:
- Forensics: After compromises, detect modifications to hardware, firmware, or logic
- Detection: Actively detect anomalies

Network monitoring alone is not sufficient to adequately defend against a sophisticated adversary.
Other ICS Cyber Security Recommendations

- Investigate all mitigation options, covering defend, detect, and manage (including incident management/recovery plans)
- Develop and install detection capabilities for attack/anomaly indicators
  - Complementary options include network traffic monitoring and advanced hardware monitoring
  - Reduce troubleshooting duration
- Develop effective environments/procedures for testing
- Minimize attacker opportunities for device configuration or firmware access (possibly disallowing such network traffic)
- Develop logic- and tamper-checking tools for devices and systems
- Focus on cyber security assessment for field devices