Improving Microgrid Cybersecurity

DLA WWEC
National Harbor, Maryland
April 11, 2017

Abraham Ellis, Ph.D.
Manager, Renewable and Distributed Systems Integration

Sandia National Laboratories
Albuquerque, NM, USA
aellis@sandia.gov
Outline

- Overview
  - Motivation and *defense-in-depth* concepts for microgrid cybersecurity

- Three ways to improving microgrids cybersecurity *
  1. Network segmentation (Microgrid Cybersecurity Reference Architecture)
  2. Hardware-based detection (WeaselBoard PLC hardware security)
  3. Better cyber-physical modeling, simulation and testing (Emulytics, SCEPTRE)

- Q&A

*Based on R&D work at Sandia National Laboratories, sponsored by:
- US Department of Energy Office of Electricity Delivery and Energy Reliability (US DOE/OE)
- US Department of Defense (US DOD)
Energy Systems and Critical Infrastructure

- Energy infrastructure is a common cybersecurity target
- Increased vulnerability due to higher utilization of industrial control systems (ICS), not generally designed with cybersecurity in mind
- Increasingly relevant to microgrids, especially critical applications

Source: US DHS ICS-CERT monitor, 2015
Source: Open-Source Vulnerability Database (OSVDB)
Defense-in-Depth Concepts

- Defense-in-depth concept
  - Multiple security layers addressing People, Technology & Operations vulnerabilities
  - Common in high security applications (e.g., DOD)

- Four stages of cybersecurity defense-in-depth
  1. Protection
     » Policies & procedures (authentication, physical security)
     » Network security (e.g., Network segmentation, encryption)
  2. Detection
     » Real-time monitoring, situational awareness
  3. Response
     » Contain consequences, impact
     » Readiness: Planning and decision support tools
  4. Restoration
     » Recover system functionality
Control System Architecture

- Room for improving cybersecurity in all layers and interfaces

- 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

Corporate Layer

SCADA Layer

ICS/Field Device Layer

Controlled Process (infrastructure)
Cyber Security Reference Architecture

- Recommendations for the design and implementation of secure microgrid control systems
  - Focus on network segmentation best practices and design criteria
  - Goal is to reduce vulnerability, consequences and recovery time
- Design process
  1. Identify all actors (microgrid operator, network administrator, corporate user, vendors, …)
  2. Describe data exchange requirements (type, volume, reliability, confidentiality, etc.) See report templates.
  3. Define enclaves with similar security and actors
  4. Define enforceable functional domains for IEDs
  5. Design and apply other cybersecurity controls (network interface firewalls, monitoring, …)
Enclaves and Functional Domains

- **Enclaves**
  - Defines a trusted environment under a single authority and security policy
  - Enclaves are selected based on common attributes for QoS, security, and data requirements

- **Functional Domains**
  - Defines allowable access and data exchange to allow actors in different enclaves to collaborate securely

Microgrid Control Network Example

- Typical control system network configuration is flat
  - Relies mostly on security policy (e.g., authentication), maybe hardening.
  - Not a good example of defense-in-depth:
    » All actors could accidentally or maliciously access all data, applications and physical assets within the microgrid
    » Potential impacts are not contained
### Data Exchange Worksheet Format

**Source:** Microgrid Cyber Security Reference Architecture V1.0, Sandia Report SAND2013-5472, July 2013

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
<th>Example Values</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Exchange</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Type</td>
<td>Type of data exchange to occur</td>
<td>monitor, control, report, write</td>
</tr>
<tr>
<td>Interval</td>
<td>How often data exchange occurs</td>
<td>e.g. milliseconds, seconds</td>
</tr>
<tr>
<td>Method</td>
<td>How data will be exchanged</td>
<td>unicast, multicast, broadcast</td>
</tr>
<tr>
<td>Priority</td>
<td>Relative importance of exchanging the data</td>
<td>high, medium, low</td>
</tr>
<tr>
<td>Latency Tolerance</td>
<td>Tolerance to delayed control or delayed data exchange</td>
<td>high (delays do not affect operation), medium, low</td>
</tr>
<tr>
<td><strong>Data</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Type</td>
<td>Type of data to be exchanged</td>
<td>voltage, setpoint, status</td>
</tr>
<tr>
<td>Accuracy</td>
<td>Necessary precision/timeliness of data</td>
<td>significant digits, time units</td>
</tr>
<tr>
<td>Volume</td>
<td>Amount of data to transferred per exchange</td>
<td>e.g. bytes, kilobytes, etc.</td>
</tr>
<tr>
<td>Reliability</td>
<td>Necessity of access to control processes and data</td>
<td>critical, important, informative</td>
</tr>
<tr>
<td><strong>Information Assurance</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Confidentiality</td>
<td>Importance of preserving restrictions to control processes and information access (based on risk to system operations and/or system security)</td>
<td>high, medium, low</td>
</tr>
<tr>
<td>Integrity</td>
<td>Importance of preventing unauthorized changes to control processes or data, including authenticity (based on reliability with respect to operations)</td>
<td>high, medium, low</td>
</tr>
<tr>
<td>Availability</td>
<td>Importance of timely and reliable access to control processes and data (based on priority and latency tolerance with respect to operations)</td>
<td>high, medium, low</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Source</th>
<th>HMI server</th>
<th>HMI client</th>
</tr>
</thead>
<tbody>
<tr>
<td>Destination</td>
<td>HMI client</td>
<td>HMI server</td>
</tr>
<tr>
<td><strong>Exchange</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Type</td>
<td>monitor</td>
<td>control</td>
</tr>
<tr>
<td>Interval</td>
<td>seconds</td>
<td>minutes to hours</td>
</tr>
<tr>
<td>Method</td>
<td>unicast</td>
<td>unicast</td>
</tr>
<tr>
<td>Priority</td>
<td>low</td>
<td>medium</td>
</tr>
<tr>
<td>Latency Tolerance</td>
<td>high</td>
<td>medium</td>
</tr>
<tr>
<td><strong>Data</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Type</td>
<td>breaker control, kW output, kVAR output, voltage magnitude and angle phase, line flow</td>
<td>breaker control, kW output control, voltage control</td>
</tr>
<tr>
<td>Accuracy</td>
<td>2 decimal places</td>
<td>2 decimal places</td>
</tr>
<tr>
<td>Volume</td>
<td>bytes</td>
<td>bytes</td>
</tr>
<tr>
<td>Reliability</td>
<td>informative</td>
<td>important</td>
</tr>
<tr>
<td><strong>Information Assurance</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Confidentiality</td>
<td>medium</td>
<td>medium</td>
</tr>
<tr>
<td>Integrity</td>
<td>high</td>
<td>medium</td>
</tr>
<tr>
<td>Availability</td>
<td>medium</td>
<td>medium</td>
</tr>
</tbody>
</table>

---
Suppose we are designing a microgrid with controllable generators, storage, and network elements managed by IEDs.

Could define 3 enclaves based on data and security requirements:

- **Operator:** Primary and backup HMIs
- **Server:** HMI server, EMS or controller
- **Manager:** Intelligent electronic devices (IEDs) controlling or managing microgrid switches, flow devices, generators, demand response, etc.

Microgrid Network Segmentation Example
Functional Domains – Examples

- IED functional domain
  - Receive data from a power device via serial connection, send *information* to EMS over TCP/IP
  - Process information from power device or from EMS, send *command* or *data request* to a power device via serial connection

- EMS functional domain
  - Receive data from IEDs, send *information* to HMI over TCP/IP
  - Process information from IEDs or operator via HMI, send *command* or *data request* to
Field Device Security

- Vulnerability of field devices (e.g., PLCs) is a challenging issue
  - Lack of situational awareness locally
  - Limited response and recovery recourses
- Sandia is working on technologies to address this gap
  - WeaselBoard: Locally monitor PLC backplane traffic in real time
  - On-board analytics to detect, alarm and block
  - Industry partnerships

Cybersecurity Analytics

- Red Team assessments and quantitative security performance scores

<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>2</td>
<td>2</td>
<td>6</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>15</td>
</tr>
<tr>
<td>Totals</td>
<td>Both</td>
<td>11</td>
<td>16</td>
<td>14</td>
<td>41</td>
<td>41</td>
</tr>
</tbody>
</table>

<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>Insecure</td>
<td>9</td>
<td>0</td>
<td>14</td>
<td>23</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>Enclaved</td>
<td>High</td>
<td>Insecure</td>
<td>7</td>
<td>6</td>
<td>11</td>
<td>24</td>
</tr>
<tr>
<td></td>
<td>Medium</td>
<td>Insecure</td>
<td>9</td>
<td>6</td>
<td>14</td>
<td>29</td>
</tr>
<tr>
<td></td>
<td>Low</td>
<td>Insecure</td>
<td>11</td>
<td>6</td>
<td>16</td>
<td>33</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Hardened</td>
<td>11</td>
<td>6</td>
<td>16</td>
<td>33</td>
</tr>
</tbody>
</table>

Maximum Possible Score → 11 16 14 41
Cybersecurity Analytics

- High fidelity, scalable cyber-physical analysis is difficult
  - Interdependent complex ICS and physical infrastructure
  - Limited capability to model ICS threats and map to physical system consequences
- Sandia’s Emulytics™ approach combines emulated, simulated, and physical testbed environments

More information:
https://vimeo.com/178492617
Emulytics: ICS Mod/Sim/Test Environment

- Model ICS devices w/ SCEPTRE
  - Remote Terminal Units (RTU)
  - Programmable Logic Controllers (PLC)
  - Protection Relays
- Model control center server/services
  - Actual SCADA/EMS/DCS software running real or virtualized hardware
- Model comms network using live-virtual-constructive approach
  - Real devices (routers, switches)
  - Emulated devices (Dynamips, Vyatta)
  - Simulated devices via OPNET Modeler
Questions? Comments?

Abraham Ellis
Sandia National Laboratories
aellis@sandia.gov