Improving Network & System Management for Substations and Field Devices

Ralph E. King
Principal Project Leader

EPRI European Engagement Summit
April 28, 2015
EPRI’s Cyber Security and Privacy Program: Cyber Security Technology Projects for 2015:

Protective Measures

Network Management Systems

DNP3 Secure Authentication v5

Managing Cyber Incidents

Integrated Security Operations Center

Integrated Threat Analysis Framework

Security Incident Management Task Force
Protective Measures: Network Management Systems

Security Monitoring
Operational Asset Health Monitoring
IEC 62351-7 MIB
Network Management Systems Research GAP!!

“IT-style monitoring of OT systems”

Control Center

Operations Network

Substation Network

SCADA/EMS

Router and Switch data to NMS = ✓

Network Management System (NMS)

IED data to NMS = ✗
Network Management Systems Research Objective: “IT-style monitoring of OT systems”

**Issue**
- Operations systems lack a scalable, vendor-neutral solution for integrated network, system, and security management.

**Project approach**
1. Develop use cases and testing scenarios
2. Vendor proof of concept
3. Utility technology transfer workshop

**Value**
- Enables utilities to more effectively monitor and manage operational systems’ health and security.
Network System Management: 2014 Project Accomplishments

- Substation Network Explorer
- Use Case Development
- Test Plan & Results
- IEC 62351-7 Development & Adoption
- EPRI Report: Implementation & Application of IEC 62351-7
- Technology Transfer Workshop
Use Cases for IEC 62351-7 explored in EPRI Cyber Security Research Lab in 2014:

**Resource Exhaustion**
- This category encompasses evaluation of machine resources and the detection of when an abnormal amount of resources are being utilized.
  - Resource Exhaustion (UC5)

**Traffic Analysis**
- The ability to use 62351-7 MIBs to determine if there is one or more different types of abnormal traffic occurring.
  - Substation Network Storm Detection and Prevention (UC2)
  - Protocol Monitoring (UC3)
  - Denial of Service Detection (UC4)
  - Traffic Pattern Analysis for intrusion detection (UC6: Login Failure)

**Component Failure and Degradation Alarms**
- This use case provides details on requirements for monitoring a component failure or impending failure.
  - Power Supply Failure (UC1)
Proposed 2015 Use Cases:

1. Implement native IEC 62351-7 MIB in network devices and IEDs
   - Accepting vendor participation!!
2. Extend Device Resource Monitoring beyond network devices to monitor IEDs
3. Monitor IED configuration changes
4. Device Clock Synchronization Monitoring
5. Perimeter Access Monitoring
7. Extend Protocol Error Detection beyond GOOSE to include DNP3
8. Send security information to SIEM using IEC 62351-7 SNMP Gateway
9. Configure other NMS to monitor IEC 62351-7 MIBs
   - Accepting vendor participation!!
Research Approach & Demonstration Environment
Research objective: Provide a scalable, vendor-neutral solution for integrated network, system, and security management by leveraging IEC 62351-7.

- Currently testing with **Eight** Network devices from **six** vendors!!
  - Most are **not** implementing 62351-7, in project plan for 2015+.
- Proof-of-concept NMS testing tool for IEC 62351-7 MIB
General Information Flow & Actors

One or more points of observation or action

IED or Intermediate Systems

SNMP subAgent(s)

SNMP Agent(s)

NSM

Analysis

Operator

Monitored Information

Monitored Information

Metric(s)

Action

Command

Commanded Action
General Information Flow & Actors (non-SNMP IEDs)

- **IED with no SNMP**
- **SNMP Proxy**
- **SNMP subAgent(s)**
- **SNMP Agent(s)**

**Non-SNMP Protocol**

**Translation to SNMP MIBs**

**Monitored Information**

**NSM**

**Analysis**

**Operator**

**Metric(s)**

**Command**

**Action**

**Commanded Action**
NMS Implementation Observations:

- The key to NMS implementation is the standard set of objects in the IEC 62351-7 MIB

- Advantages of NMS in the utility sector are obtained by utilizing the MIB with new or existing NMS tools

- The MIB is not limited to substations but can be expanded to any environment

- The MIB is compared/mapped to other standards in the report
  - ISO FCAPS (Fault, Configuration, Accounting, Performance, Security)
  - Information Technology Infrastructure Library (ITIL)
  - IEC 61850
  - SNMP
Substation Network Explorer (SNE) Proof-of-Concept Testing Tool:

HMI for Use Case Testing and Demonstration

Developed in EPRI Cyber Security Research Lab

Monitors & Reports on IEC 62351-7 MIBs

Available for vendors and EPRI members for testing
Current Proof-of-Concept Capabilities:

- Network Topology
- IED Configuration
- Key System Resources
- CPU/Memory/Temperature
- Power Supply
- Network Visualization
- Asset Health & Security Monitoring
- Network Performance Analysis
- Deep Packet Inspection of Network Traffic
- Industry First IEC 62351-7 SNMP Gateway
- Report all Security Objects in IEC 62351-7 MIBs
- Convert Vendor Specific MIBs to 62351-7 MIBs
- Supports Multiple NMS Masters
- Package Device or Major Header Detection
- Report all Security Objects in IEC 62351-7 MIBs
- Convert Vendor Specific MIBs to 62351-7 MIBs
- Supports Multiple NMS Masters
- Package Device or Major Header Detection
Substation Network Explorer Software Architecture: Power Supply Failure Example

**Visualization GUI**

**Substation Model/Traffic Analysis Module**

**SNMP Server**

**SNMP Gateway**

**Lost PS-A**

**Event 1**
- PS-1 Failure
- *SNMP Trap Event*

**Event 2**
- PS-1 Failure
- *IEC 62351-7 Event*

**Power Supply Failed!**

**SNMP Trap**

**Network Monitoring**

**SNMP Poll**

**Switch**

**NMS Server**

**62351-7 SNMP**

**SIEM**

Or Control Center NMS
Substation Network Explorer
IEC 62351-7 MIB

Demonstration
SNE Demonstration – Areva Relay Power Loss
SNE Demonstration – Cisco Switch Power Loss
Network System Management: Proposed Objectives for 2015

- Configure and test the current Substation Network Explorer NMS tool at a member utility

- Advanced use cases
  - Monitor configuration changes in IED’s
  - Extend Device Resource Monitoring beyond network devices to monitor IEDs

- Additional vendor integration in the Cyber Security Research Lab:
  - With additional vendor NSM solutions
  - With additional vendor IEDs (moving towards native implementation of IEC MIB)
    - MIB is freely available!
# 2014 Cyber Security Technologies Reports:

<table>
<thead>
<tr>
<th>Report Title</th>
<th>Product ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>DNP3 (IEEE Std 1815TM) Secure Authentication: Implementation and Migration</td>
<td>3002003736</td>
</tr>
<tr>
<td>Guide and Demonstration Report</td>
<td></td>
</tr>
<tr>
<td>Network System Management: Implementations and Applications of the IEC 62351-7 Standard</td>
<td>3002003738</td>
</tr>
<tr>
<td>Guidelines for Integrating Control Center Systems Into an Integrated Security Operations Center</td>
<td>3002003739</td>
</tr>
</tbody>
</table>

### How to download EPRI Reports:

1. Go to [www.epri.com](http://www.epri.com)
2. Type the Product ID in the Search Bar
Together…Shaping the Future of Electricity