

Industrial Control System (ICS)
Asset Monitoring and Status:
A Proposed Solution Architecture

Joe McCormick, Data Track Technology

James Moralez, SDG&E

ICS Asset Monitoring Today

- It is, generally, a labor-intensive and manual process:
 - Dispatch an engineer to the remote site with appropriate access.
 - Capture essential asset inventory information in paper or electronic form, depending on systems that may be available.
 - Print and archive information in both a paper form and, perhaps, in a simple database system.
 - Repeat as necessary.
- These snapshots of asset inventory information are referenced as necessary, but may be out of date within weeks.
- It is difficult to know that the configuration and connectivity status are still accurate when viewing the data.
- This is a process ripe for automation and advanced systems support, particularly since the data is essential for security.

Problem Definition via DHS

- Department of Homeland Security document Roadmap to Secure Control Systems in the Dams Sector, December 7, 2009 - Draft Version 3:

“Currently, asset owners and operators do not have adequate inventories of their critical assets and associated ICS or a good understanding of the risks (threats, vulnerabilities and consequences) of a cyber attack. The growing number of nodes and access points has made identifying vulnerabilities more complex. Widely accepted industry standards, consistent metrics and reliable measuring tools are not readily available; however, they are essential to assessing the security/risk of these increasingly complex control systems and all of their components and links.”

Problem Definition via NIST

NIST Special Publication 800-82, Guide to Industrial Control Systems (ICS) Security,

Table 3-5 (Platform Hardware Vulnerabilities):

“Undocumented assets – To properly secure an ICS, there should be an accurate listing of the assets in the system. An inaccurate representation of the control system and its components could leave an unauthorized access point or backdoor into the ICS.”

Table 3-4 Platform Configuration Vulnerabilities:

“Critical configurations are not stored or backed up – Procedures should be available for restoring ICS configuration settings in the event of accidental or adversary-initiated configuration changes to maintain system availability and prevent loss of data.”

Problem Analysis

- Gaps will exist in understanding what the effects of an intentional—or “unintentional”—cyber attack or event on an ICS will be without essential asset inventory information being updated dynamically and accurately on a regular basis.
- This essential asset information includes configurations, communication interconnections, communication status, and device status of each component within the ICS.
- An automated solution for monitoring configuration and status changes in the individual ICS devices is an essential element of a security strategy, and will greatly contribute to the overall situational awareness of the entire ICS.
- The more robust the solution, the easier it will be to prevent or mitigate the effects from an attack, a mis-configuration , or an equipment failure within the ICS.

High Level Requirements (1)

- Deliver another dimension of situational awareness of an ICS by monitoring essential asset inventory information in light of security concerns.
- Create a “network” management system—independent of SCADA interfaces—where a distributed ICS can be automatically and remotely monitored for configuration changes, connectivity, and device status.
- Architecture, System Features, and User Interface should rival the quality of the best commercial off-the-shelf (COTS) network management systems:
 - Relational Database Management System (RDMBS) for data storage
 - Rule-driven, dynamic analytics for information processing
 - Browser-based “dashboard” technology for actionable presentation

High Level Requirements (2)

- Handle legacy systems either in place, or being migrated to “smarter” systems, e.g., substation automation within the electric grid.
- Connect to ICS devices via agents (Local Monitor) within secure access control gateways. Use a direct connection interface port, secure modem, or an Ethernet (TCP/IP) interface on each device to be monitored.
- Employ scalable, distributed intelligence within the solution where the Local Monitor will capture, analyze, and possibly react to the data; compress and encrypt them; and then forward them to a Central Monitor server.
- Monitor ICS assets from multiple vendors to support heterogeneous environments.

General Feature Categories

- Perceived need and high-level requirements drove the following feature categories for an automated system:
 - ICS asset configuration management
 - Compare the latest configuration scan data to the previous configuration scan data, highlighting any changes.
 - Present the history of configuration changes to each device and all devices within the entire ICS.
 - ICS asset maintenance connectivity status
- Feedback from several utilities in the electric sector on the core ideas drove another feature category:
 - ICS device status
 - Capture the output of specific device status commands.
 - Analyze the output for both current and historical significance.
 - Present the analysis in an actionable form.

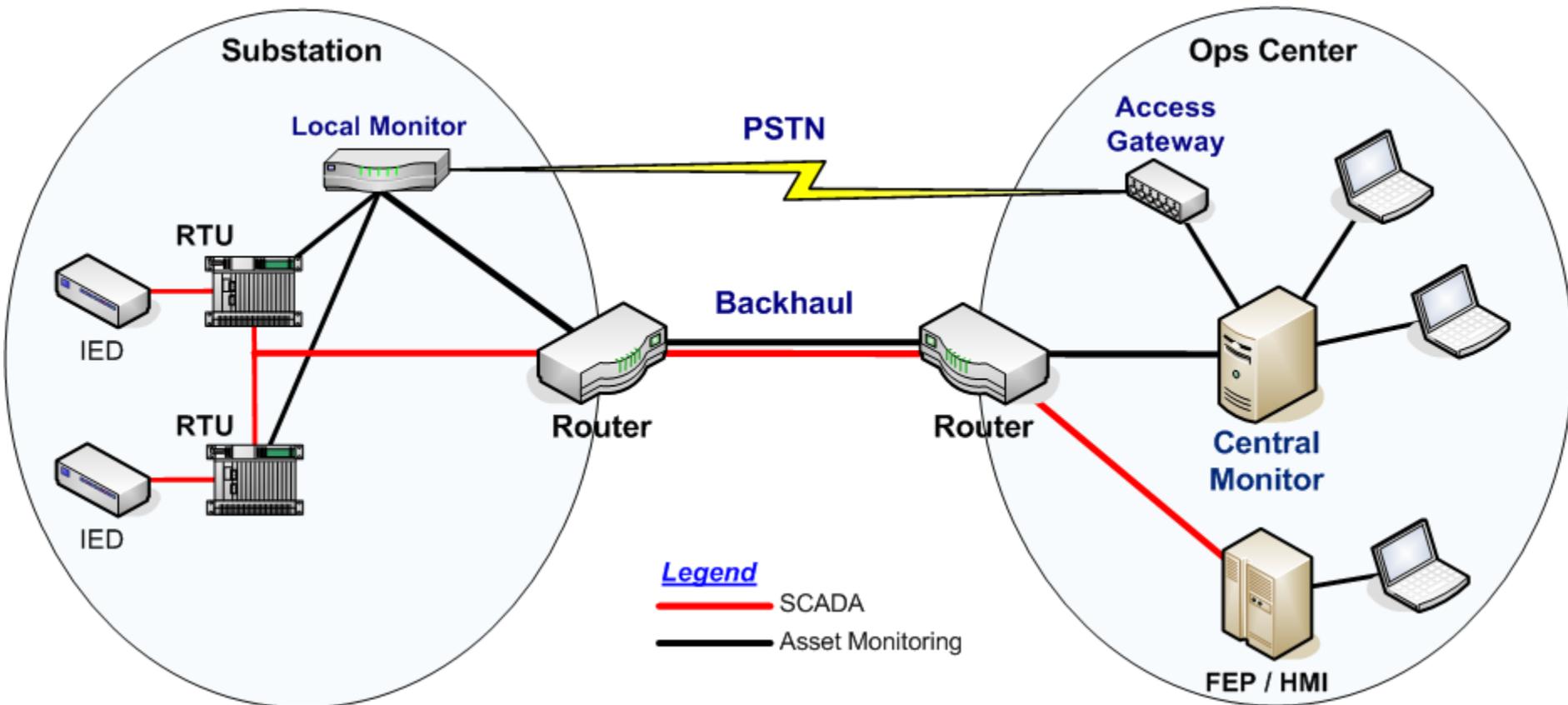
Detailed Requirements (1)

- Scan using a series of defined intervals for gathering the various sets of data. Intervals will be set from within the software, and be based on asset owner policy.
- Support existing control devices (RTU's, PLC's, IED's, etc.) with maintenance or console port interfaces (preferred), or through interleaving communications between polling cycles on an active port.
- Of course, there must be seamless support for new control devices with Ethernet interfaces using TCP/IP protocols.
- There should be no difference to the user interface or to the system analysis because of possible differences in the connectivity technology that inter-connect devices down to the lowest level of device chaining.

Detailed Requirements (2)

- 3 major inquiries an ICS asset monitoring system must determine:
 1. What changes have taken place since the last scan?
 2. When did the changes take place?
 3. Who made the changes?
- Perform system functions both locally to the assets, i.e., within the Local Monitor on site, and also more advanced system functions within the Central Monitor server.
- Minimize bandwidth requirements needed between the remote locations and the Central Monitor by compressing and forwarding only the data essential for analysis in order to best support environments with limited backhaul networks.

Example: Electric Grid Substation



Audience Participation

➤ Questions

➤ Comments

➤ Recommendations

Contact Information

- Joe McCormick is a Product Manager with Data Track Technology, a company that develops communications management and SCADA solutions for utilities, carriers, manufacturers, and enterprises. Joe can be reached at jpm@moonframe.com.
- James Moralez is a Senior Engineer working in the System Protection and Controls Engineering group at San Diego Gas & Electric. James can be reached at james-pe@earthlink.net.