Connectivity 101 for Remote Monitoring Systems

Paul Wacker  
Moxa, Inc.  
Manager - Edge Connectivity

Ariana Drivdahl  
Moxa, Inc.  
Product Marketing Manager
Pain Points of Remote Monitoring

Pressure to enhance overall productivity and prevent unplanned downtime

An identified need for a single go-to-source for all connectivity requirements

Unreliable access to devices in harsh or mobile environments

The total burden of risks, involving security issues.

Interoperability and scale of the existing infrastructure cannot accommodate the escalating demands in an ever-transforming operational milieu

Deploying connectivity infrastructure is a complex and time-consuming undertaking
Choose the Right Communications Protocol
Traditional “Pollled” Architecture

Field Devices

→ Request
← Response

Poll Cycle Time

\[ \text{#Sites} \times (T_{\text{SEND}} + T_{\text{PROC}} + T_{\text{RECV}} + T_{\text{DELAY}}) \]
Limitations of Polled Systems

• Sequential processing
  – Poll cycle time proportional to device count
  – Impacted by data size, response time, faults

• Data considerations
  – Field devices must be polled, even if data doesn’t
  – Update rate limited by polling period

• Operating costs (cellular/satellite)
  – Usage based pricing ($/MB)
  – Impact on data point count
  – Impact on polling rate
“Report by Exception” (Data Change)

• ‘Active Tags’
  – Digital: Send on change (e.g. Off → On)
  – Analog: Send on percentage (%) change
  – Optional: Refresh on specified interval (sec.)
“Report by Exception”

Data “pushed” on change

- Minimizes data transfer
- Faster data updates
- Firewall “friendly”

いますが、少数のフィールドデバイスがサポートしています
Emerging Technologies …

MQTT: Message Queuing Telemetry Transport

http://mqtt.org/
Be Prepared for Devices Utilizing Different Protocols
Handling Different Protocols

• Passive
  – Transparently tunnel serial data over IP
  – RS-232 to Ethernet

• Active
  – Optional CPU with secondary interface
  – Accessory plug-in module (3rd party)
  – Embedded PC
  – Industrial gateway
Serial-to-Ethernet

- Connects serial (RS-232/422/485) devices to Ethernet
- Serial data is encapsulated in IP “packets” for transport over the network
- Known as “Device Server” “Serial Server” or in IT as a “Terminal Server”
- Transparent to attached devices and application software
Industrial Ethernet Gateway

• Specialized Device Server
• Translator for different devices
• Utilizes “shared memory”
  – User configured polling table
  – Can be client or server
Active Gateway Operation

Active “polling” refreshes internal Data Tables

Input Table
Output Table

Request
Response

Internal Data Tables

Modbus
EtherCAT/IP

Request
Response
Expect Communications Disruptions
Secondary/Backup Network

- **Backup**
  - Redundant connections
  - Secondary network provider(s)
  - Requires managed switch or router

- **Cellular modem/router**
  - Signal coverage
  - External antenna/placement
  - Monthly service fee
  - Usage fees (per MB)
Cellular: Connection Recovery

- Rapid recovery minimizes data loss
- Requires progressive approach
  - Cellular reconnect
  - Reset cellular
  - Device restart
Cellular: Carrier Failover

- Backup cellular communication
- Keeping device always online
Data Buffering

• **Useful for streaming serial data**
  – Serial: RS-232/422/485
  – Scales, barcode scanners, etc
  – Environmental sensors

• **First In First Out (FIFO)**
  – Data is buffered on network loss
  – Local data storage (SD card)
  – Push data on network reconnection
Offline Storage (Data Logging)

- Capture process data
  - Internal storage (NVRAM)
  - Expandable storage (SD card)
- Date/time stamp (real-time clock)
Local/Offline Control

- Consider operational and safety issues
  - Controlled shut-down on network loss
  - Stand-alone or autonomous operation

- Local control options
  - Simple sequencing and logic
  - Built-in to field device (PLC, RTU)
  - Add a “smart connected relay”
Design-in Security from the Start
“The reality is that security is not something you can buy; it is something you must get.”

Bruce Schneier
Renowned Security Technologist
Industrial Systems are in the Crosshairs

No Vendor or user is immune from a potential cyber security incident

Source: Honeywell Cyber Security Lab
Increasing Incidents, especially in Critical Manufacturing

- **2013**
  - Energy Sector: 257
  - Critical Manufacturing: ↓ 46%

- **2014**
  - Energy Sector: 245
  - Critical Manufacturing: ↑ 71%

- **2014-2015**
  - Energy Sector: ↓ 42%
  - Critical Manufacturing: ↑ 49%
  - New: Water, Transportation: ↑ 50%

- **2015**
  - 295
Best Practice to Decrease Cybersecurity Risk

Plant security
• Block access for unauthorized persons
• Physical prevention of access to critical components

Network security
• Strictly control interfaces between office and plant network (e.g. via firewalls)
• Segmentation of plant network (e.g. VLAN or subnet segment)

System Integrity
• User authentication for plant or machine operators
• Antivirus software and whitelisting policy for control servers
• Maintenance and update processes for vulnerability patch
• Access protection mechanisms for automation components
Defense-in-Depth Strategy

• Employ life-cycle processes
  – Threat assessment
  – Implementation of countermeasures
  – Monitoring and maintenance

• Network segmentation
  – Break down to physical/logical zones
  – Group by security requirements
  – Clearly define borders
  – Identify connections between zones

• Define Zone to Zone interaction
  – Determine device requirements
  – Identify allowed traffic
Application: Secure Pipeline Monitoring

Firewall / VPN
Firewall: Basic Operation

**Firewall Policy:**
- Incoming/outgoing
- IP/MAC
- Protocol (TCP, UDP…)
- Source IP/Port
- Destination IP/Port
Firewall: Policy Processing

- Policies are stored in lists
- Checked sequentially until matched
  - List ‘accepts’ first
  - End with ‘drop’ all

Best Practice: Always use a Positive Listing, dropping all but specified traffic.
VPN: Virtual Private Network

- Extends a private network across a public network
- Virtual point-to-point connect with encryption
VPN Key Features

• Secure ‘tunnel’ over un-trusted networks
  – IPSec
  – OpenVPN

• Allow only authorized users
  – Password or digital certificate
  – Centralized server (RADIUS)

• Ensure data integrity
  – Confirm data source
  – Confirm data has not been altered

• Hide in-transit data (encryption)
VPN: Common Use-Cases

• Remote Access

• Site-to-Site
Select Infrastructure that supports Remote Monitoring
What do you do when …

- Your SCADA/HMI shows a device offline
- Your PLC shows an Ethernet remote I/O fault
- You’re having SCADA communications faults
SNMP: The ‘IT” Solution

- Simple Network Monitoring Protocol (SNMP)
- ‘Modbus of the IT world’
- Framework that provides facilities for managing and monitoring network devices
  - Agent
  - Manager or Network Management System (NMS)
  - Management Information Bases (MIBs)
Device Health/Status Monitoring

- System status
  - Power (Pwr1, Pwr2)
  - System faults
- Ethernet port status
  - Up/Down
  - Speed (10/100/1000 Mbps)
- Traffic (packets) monitoring
  - Sent
  - Received
  - Errors
- And much more …
Monitoring your Infrastructure

• Conventional Approach: SNMP

• Native Industrial Protocol Support
Network Management & Maintenance

Network Management Software
- Topology visualization
- Remote device management and configuration
- Real-time event management
- Performance reporting
Network Management & Maintenance
Efficient Visual Monitoring

Virtual Device Panel
Visualization
Real-time Event
Remote Monitoring on your phone!
Industrial Network Management Software in Your Pocket

- Real-time Notifications
- Network Status Check
- Easy Device Mapping

Available on the Google Play and Apple App Store
Thank you!