Requirements and Scenarios for Industry Internet Addressing

draft-km-industrial-internet-requirements-00

K. Makhijani, L. Dong

IETF 111 (INTAREA – July 30 2021)
Motivation

• Introduction to Industry Control Networks
• Scenarios & Challenges from emerging trends
• Possible functional areas to progress
Industry Control Networks

The Business logic ➔ over Internet Protocols
IP/TCP.
E.g., supply chain, quality assurance, inventory management, sales, etc.

The Operations ➔ over Industry Network Protocols
E.g., Manufacturing sites, plants, production sites, agriculture, factories, etc.

Automation = Connectivity of \{OpsTech\} + \{InfoTech\}
Properties of the Industrial Networks

• Wired devices:
  • A bulk of machines are over wired network;
  • Constraints vary from commercial IoT devices related work.
  • Device lifetime, or power-requirements are not typical constraints.
  • Instead, direct process control loops are more important.

• Location, Zone Specific:
  • Device specific location changes are rare.
  • Highly engineered - the network resources get efficiently utilized.

• Security by separation:
  • Typically, attack vectors are minimized by separating IT infrastructure from OT.

• Communication patterns:
  • Client server, sensor data, actuator data, app specific data etc.

• Time centric behavior:
  • The control devices requiring deterministic behavior covered under the DetNet.
Scenarios

1. **OT/IT Convergence**
   - Decisions to move IT servers on factory floors or transport data out of the floors.
   - Overheads relating to IP headers not suitable for Industry protocols.

2. **Virtualization**
   - Of processes, PLCs to make them location agnostic
   - Digital Twin instances from underlying collection of devices.

3. **Implications of Data growth from new use cases**
   - Compute intensive scenarios
     - E.g., use of cameras installed for visual inspection to determine the quality of manufactured product generates a high bandwidth demand.

4. **Variety of Infrastructure Networks**
   - Factory infrastructure + Building automation - lights, A/C, thermostat control
   - + floor safety and security infrastructure
Challenges with the current state

• Dealing with Heterogeneity of Industry Protocols
  • More than 100 protocols: controller sits behind one protocol and control devices behind the other protocols.
  • Stateful gateways for translations.

• Automation Impact
  • Scale – Automation adds more sensors, more data on the wire. This stresses the ‘engineered networks’ by making them more compute and data intensive.
  • OT Fabric stretch to Edges or Clouds – moving from hardware PLCs to software or virtual PLCs.
  • Must achieve same level of reliability and resilience as factory floor (on-prem).
Structural Differences in Addresses

- **IP Address**
  - Fixed number of bytes that identifies a node

- **Industrial Protocols**
  - Different process control zones have their own address space
  - Do not have a network layer (LAN scoped control area)
  - Protocol format conversions happen on the fly - devices of one protocol often connect to controller of other protocols
Simplify OT/IT Integration

IP Technologies

Applications Network

Industrial (Process control) Technologies

Data
Addr-Func
PHY

serial bus

BacNet MS/TP (Net-A)

Ethernet

BACnet/PDU

IP

Ethernet

PHY

Profibus (Net-D)

serial

Modbus (Net C)

BACnet/PDU

PHY

SA-DA-FC

IP nodes

Ind-device A

Ind-device B

Some new kind of structure

IETF 111 - INTAREA - Industry Network Scenarios
Potential work-areas

• Device side of work - Common Network format which is friendly to both OT and IT applications.
  • Typical actuator and sensor data is small
  • Evaluate compressed header SCHC, ROHC (?)
  • Or a newer flexible address structure.

• Network Layer for Industrial Devices
  • One device address for an industrial device is the same at PHY, MAC and application level.
  • Use case: with virtual PLCs, need for more qualified address of the device.
  • Gateway simplification – with more context in the network layer.

• Network specific work - Encap-free communication between devices with different address schemes
  • Short Device addresses on the wire (today fieldbus address are 1-byte, to have uniqueness, it needs to be coupled with some semantics – such as location, controller, applications, etc.)
Next Steps

• Address-Framework
  • Format of reachability on wire
  • Support different addresses family/spaces?
  • Using “something-over-IP” (encapsulated over IP) has its own cost, translation overhead and complexity.

• IOTOPS WG
  • Possible place holder for driving discussions on setting up the framework and requirements

• Inviting contributors and reviewers

Thanks!

Comments and feedback

IETF 111 - INTAREA - Industry Network Scenarios