Early-stage approach to Integrated Industry Network Framework

draft-iotops-km-iiot-frwk-00

Kiran Makhijani

Lijun Dong
Based on discussion @111, we started a new document to describe details of the framework

- Admittedly, might have mixed up the current framework vs what it *Should be*
  - draft-km-industrial-internet-requirements-00 was more specific; we would continue to improve it.

Still a high level with lots of open questions

- Purpose is to evaluate can we use this as a reference for coordination with IIoT domain experts.

- Of course, invite collaboration, coauthors and reviewers.
Motivation
To what extent, how and where IETF technologies can be leveraged for IIoT?

• Better OT/IT integration – Application to Device
• IIoT Cloudification implications
  • Extension of OT networks to edge or cloud
• Multiple Media - different technologies
  • Potential transition to Ethernet but right now all types of Fieldbus protocols exist.
  • Special functional significance embedded (time-sync, bandwidth).
• Virtualization of PLC
• Devices interact with more than one applications
What's in the Framework

1. Integrated Industry Network (IIN)
   • Design and technical requirements
   • From device side as well as networks nodes

2. Infrastructure (limited-domains model)
   • Interconnection between public and ‘special purpose’ networks
   • using LDN architecture/nomenclature (RFC 8799).
   • Focus is to stay aligned with Industry control architecture

3. Cooperation with IIoT focus consortia
   • Identify organizations involved and relevant scenarios
OT: Reference ISA 65 Architecture

Enterprise Security Zone:
• Typical IT applications perform tasks necessary for business operations such as inventory control, supply-chain logistics, schedule and capacity planning.

Industrial Demilitarized Zone:
• An information sharing layer since OT and IT networks were designed to prevent direct communication between them.
• Translation of security rules, inspection and protection of device identity and access is necessary when transiting from to L4.

Manufacturing Zone:
Levels 0 through 3 site wide production system.

Note: attention to boundaries across different levels:
• Enterprise, IDMZ, Industry security zones.
• Good starting point, even though it is manufacturing centric
Interfaces Industry Network Framework

- Derived from LDN Structure and integrated with Purdue Model.
- Constraints:
  - Maintain the level discipline. i.e., only allow in-order communication from lower to upper levels.
  - Handling for cloud and edge cases.

**Lx**: levels  
**BP**: Boundary Protocols  
**IINS**: IIN stack

Placements:  
*(Lx..)*: Levels in a zone  
*+L1,L2,..+:* cloud/edge new placements

---

**Limited-Domain 8799**  
**Outside**: public Internet based  
**Inside**: Local choices, closed administration  
**Boundary**: translations for format, security etc.
OT Networks

Network architecture for Inside protocols
- **App level processing**: IP is used as transport. Intra-zone (IDMZ) or Inter-zone
- **Security by separation**: firewalls between the zones. Lots of rules provisioned to firewalls and it will challenge the scale as number of sensors added to network grow.
- **Scale of the networks**: Even if we assume the networks are designed with TSN and Detnet additional segmentation on services, cells will be needed to provide network level support – who can access what and how the data flows.

There are many more layers
What an Integrated Industry Network could look like?

Local Management
- Localized with zone awareness.
- manage both IDMZ and factory zones
- Provisioning and Device registration
- Gateway policies

Local Control Components
- Dynamic reachability methods
- FIB population/protocols (IGP)
- Detnet and TSN aware controls

Local Data plane
- Normalized for different media buses
- Encapsulation free from app layer
- Communication pattern aware
Requirements for IIN – Device Side

• What is an endpoint?
  • Virtual PLC, Digital twin instance, Physical PLC or an attached fieldbus/ethernet device?
  • Device identification (location, virtual) and authentication.
  • Is PLC (level-1) functions as an endpoint or a network node w.r.t level 0?

• Device address assignments and management
  • Devices are associated with controllers. Part of the address/identification is ‘pre-set’ or static.

• Trust devices vs the source where commands to devices are appearing from
  • Some command authorization mechanisms
Requirements for IIN – Network Side

• Integrate data plane
  • How do we adopt different protocols and their properties?
    • SCHC inspired data plane – but cannot use as is since Rule IDs wont scale well.
    • Context: additional context for service or consumers (pub/sub – OPC-UA or Detnet type control word).
    • Efficiency – since the amount of data generated is only going to grow.
    • Virtualization, segmentation, isolation, gateway simplification

• Design for safety
  • Leverage IETF solutions and factory use case – detect and report anomalies in traffic pattern. draft-zhou-nmrg-digitaltwin-network-concepts-05
Requirements (Contd.)

• Domain specific Functionality
  • Mechanisms for boundary translations (inter-site connectivity)
  • Ingress, egress policies on traffic in each zone
    • Secure transfer of information across the zones
  • Stateless zone-specific firewalls
Working with Stakeholders

• IIC: Will provide a lot of opportunities for coordinating requirements
  • rich resource of use cases and organizations involved in OT development

• OPC-UA: provide an abstraction of data.
  • could certainly benefit from communication technologies

• IEC/IEEE 60802 project: Partnership between OT and IT.
  • Working on different profiles related to integration with OT scenarios.

This is the last slide -- Thank you for your attention --- look forward to discussion and feedback