Workgroup: Independent Submission
Internet-Draft: draft-iotops-km-iiot-frwk-00
Published: 25 October 2021
Intended Status: Informational
Expires: 28 April 2022
Authors: K. Makhijani Futurewei
L. Dong Futurewei

Framework For Integrated Industrial Networks

Abstract

Industry control networks host a diverse set of non-internet protocols supporting Industrial-IoT and legacy device connections. The integration between traditional information technology (IT) and operational technology (OT) so far has centered around collection of real-time data from devices in OT environment for consumption within the enterprise IT networks. However, improvements in process control and automation require a far better interworking between the OT and IT applications. This document provides a reference framework for integrated industry networks (IIN). It highlights interfaces and their characteristics required for interconnecting components of OT and IT that maybe moved to the cloud or edges. It suggests the use of IIN to bridge the differences between OT and IETF technologies.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on 28 April 2022.

Table of Contents

1. Introduction

There is very little cross-over between the network technologies used in the OT and IT environment. The OT networks are responsible for automation and process control on premises such as factory floors, manufacturing plants, power grids, oil & gas industry, etc. In contrast, IT networks traditionally facilitated business applications based on data received from OT applications. With increased automation, and growing demand for remote operations, it is imminent that the two technology domains need to interwork seamlessly and reliably.

Due to lack of coordination between industrial networks and IETF technologies, their evolution priorities have been different and as a result, current IETF technologies and protocols are not well adapted in industrial networks. Industrial systems and applications are becoming increasingly complex and proprietary as emerging use cases require a higher integration of OT-IT functions.

The OT networks are often tied to a set of non-internet protocols such as Modbus, Profibus, CANbus, Profinet, etc [SURV]. There are more than 100 different protocols each with it's own packet format and are used in the industry. On the other side inventory management, analytics, monitoring, supply chain and simulation software are part of IT and use IP based technologies.

> Note: use IETF technology (instead of IP-based) as a more inclusive term.

No two industry sectors are same and present different requirements and challenges on the networks. These differences are even more enhanced in industry automation and operations. The processes, control operations, environmental conditions, frequency and type data collection vary across each sector. Yet, there is a need for common, interoperable, off-the-shelf mechanisms and protocols so that applications can be deployed in relatively shorter time.

> Note: maybe later describe examples from different sectors. e.g. petrochemical or mining plant vs manufacturing and transportation. or simply refer to IIC case studies.

This document provides a framework called 'Integrated Industrial Networks' (or IIN for short) and a discussion on integration of process control, monitoring and operations with IT. It proposes (a) an idea about integrated industrial network stack that would support functions and capabilities from both OT and IT systems, (b) a structured deployment considerations, (c) alignment and coordination across stakeholders from other consortia and SDOs.

2. Terminology

Industrial Control Networks:
The industrial control networks are interconnection of equipments used for the operation, control or monitoring of machines in the industry environment. It involves different level of communications - between field bus devices, digital controllers and software applications

Industry Automation:
Mechanisms that enable machine to machine communication by use of technologies that enable automatic control and operation of

industrial devices and processes leading to minimizing human intervention.

Control Loop:
Todo

Feedback Control Loop:
Todo

Programmable logic controllers (PLC):
Industrial computers/servers for the control of manufacturing processes such as assembly lines.

Supervisory Control and Data Acquisition (SCADA):
Software System to control industrial processes and collect and manage data.

Distributed Control Systems (DCS):
Systems of sensors and controllers that are distributed throughout a plant.

Manufacturing Execution System (MES):
Systems that connect production equipment across the factory floor, or multiple plants or sites.

Fieldbus Devices:
Operational Technology field devices include valves, transmitters, switches and actuators etc.

Integrated Industrial Network (IIN):
The term introduced in this document to represent a converged view of OT and IT networks.

2.1. Acronyms

*HMI: Human Machine Interface

*MES: Manufacturing Execution System

*IIN: Integrated Industrial Network

*IIC: Industrial Internet Consortium

3. High Level Considerations

In this framework a greater focus is on capturing functional and operational requirements for the emerging use cases. The top three considerations are - first, to identify the components required to fulfill the needs for both IT and OT applications. Second, Integrated Industrial Network (IIN) Framework needs to meet and adapt to evolving deployment strategies that include cloud and edge technologies. Finally, mechanisms to coordinate with stakeholders (domain experts) should also be identified when discussing such a framework.

3.1. Integrated Industrial Network Stack

Industrial Networks are a combination of technologies that provide capability for the delivery of process control data to/from (and across) the machines and sensors to different controllers and other application specific servers. Thus, in IIN stack, one end often be an OT device and other end an IT function.

In OT Systems traditionally,

- *Operations or tasks are Well-defined: the emphasis is on having specific set of tasks performed with definitive outcomes and behavior.

- *Safety is paramount: protecting and preventing the state of the system from potential harm or disruption. The requirements in networks translate to multiple attributes such as each signals to shut off a valve are received in predictable (or real-time) and are never lost.

In addition, there is also an emergence of new use cases and scenarios in OT:

- *Multiple applications: Number of use cases are increasing from traditional deployments. A plant may need different industry protocols for different use cases. For example, BACNet for building automation, ModBus devices for valve or pressure control, ProfiBus IP for surveillance.

- *Virtualization: The role of software PLCs is growing. When met with specific time-specific constraints, virtual PLCs can operate on actuators and sensors as well as physical PLCs. In addition they can be extended to support rich set of new functions controlling different type of end devices from a single PLCs. Not to mention systems such as SCADA, MES, HMI and ICS are also being virtualized and can be deployed and operated in distributed fashion.

- *Analytics: New kinds of sensors are being deployed to monitor the health of the equipment and environmental conditions. The data collected from sensors helps in predictive maintenance, changing production schedules etc.

- *Simulation models: TBD.

- *PLC and OT Cloudification: Due to virtualization of components, it is now possible to place them anywhere in edge or cloud depending on the application design.

Some of the reasons why leveraging IETF technologies would be beneficial:

*Scalability: IETF solutions are designed for scale and perform well when dealing with large-scale network connectivity and reachability.

*Monitoring: Available solutions for health, operations and management of the network devices.

*Security: Comprehensive set of security solutions (at least in IT applications).

Note: we can add more details on routing, device and service discovery or even transport.

See Section 4 for details.

3.2. Deployment Considerations

A conceptual industry adopted reference model for network segmentation is known by Purdue model or ISA-95 [ISA95]. It shows hierarchical levels through which ordered connectivity between the components (or entities) in Industry Control Systems (ICS) is established. These levels range from 0 at the lowest level for the physical devices to applications at level 5. Those levels also include other control and management equipments (potentially treated as in-network functions and capabilities).

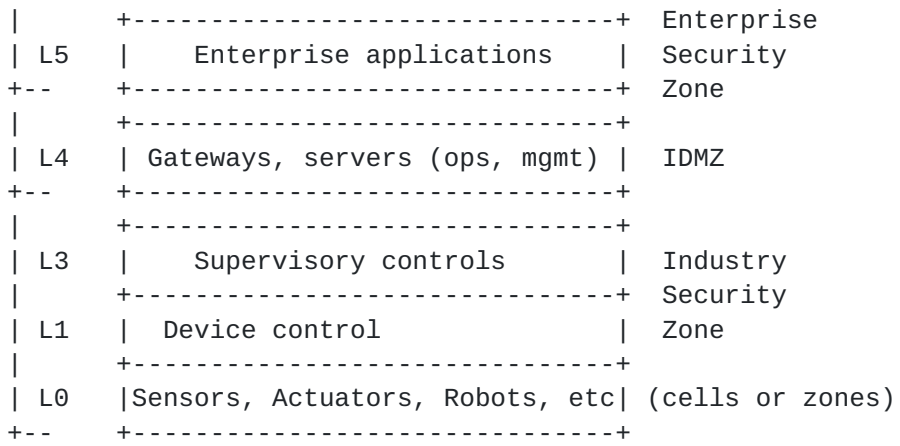

Figure 1: ISA 95 or Purdue model of Automation Pyramid

The scope and functions in each zone in [ISA95] are summarized below:

*__Enterprise Security Zone:__ The IT applications reside in enterprise networks and perform tasks necessary for business operations such as inventory control, supply-chain logistics, schedule and capacity planning. They need to collect data from the OT systems in order to make those decisions.

*

Industrial Demilitarized Zone: The OT and IT networks were designed to prevent direct communication between them. The IDMZ serves as an information sharing layer between the IT and OT (L4 and L3) systems. This indicates that additional security rules, inspection and protection of device identity and access is necessary when transiting from L3 to L4.

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

  - Site operations (L3): Supports side-wide view of the production system. Also provide data to L4.

  - Area supervisory control (L2): Performs operation and control over a zone or smaller area in a production floor. Each area has specific set of tasks or operations to perform.

  - Basic control (L1): For the actual control of the equipment. L1 components send commands to L0 equipments to perform tasks (e.g. start motor, alter pressure level, or reduce motor speed).

  - Process(L0): Level for the process equipments performing actual operations are performed. This include equipment and devices such as motors, pressure valves, temperature, speed, etc sensors, etc.

3.2.1. Limited Domain Network Inspired Framework

Effectively, industrial networks are under a single administrative control or a limited group of administrators. They are expected to extend across different geographies and over a range of distances.

RFC 8799 [LDN] introduces a formal structure and taxonomy to describe large-scale private networks called limited domains. LDNs use public Internet for connectivity across multiple sites and adhere to Internet protocols. However, with in a site, it is acceptable to use proprietary protocols. Thus, an LDN comprises of Internal, External and Boundary protocols.

Industrial networks also extend to multiple sites. The enterprise services will reside in the cloud or edges, while factory floors or plants are at remote locations. Structurally, ISA architecture (Figure 1) can be expressed as IETF's Limited Domain Networks [LDN] framework. Thus, L4 and L5 levels in enterprise zone are one site, connected via global Internet to L3-L0 levels at factory floors or plants. Using LDN model, we get break down the framework requirements systematically:

* **Inside Network Requirements (manufacturing zone)** Inside networks support OT specific protocols and maybe combination of IP and non-IP solutions. This may utilize encapsulations in IP,

compression of headers in IP or new native-short header approaches.

* **Outside Network Requirements (global or public Internet)** External public networks will interconnect different sites using IETF technologies of the Internet. These may utilize pure IPv6, NAT, VPNS or similar technologies.

* Boundary Network Requirements - for translations between inside to outside protocols.

Note: LDN is a methodology that helps in defining deployment boundaries (how, what, where) between the use specific protocols in a network-zone. it is specifically interesting here because of 2 reasons - as virtualized components move from one site to other security, safety and data-privacy perimeter changes. We need to make sure proper security profiles get applied. Secondly, it especially aligns well with the border protocols mapping to the IDMZ definition in Purdue model. There is one problem though - instinctively, we see edge services located in boundary protocols (or in IDMZ) not as a separate site. So RFC8799 needs to say more than translations about the border protocols.

3.3. Alignment with stakeholders

The paradigms of networking in OT are quite different than IP based best-effort networking protocols. Yet, IETF protocols are extensively used in OT applications. Often, it is not possible to get contributors directly from the OT sectors, then it would make more sense to coordinate with well-established consortia where OT scenarios and requirements are is discussed may be utilized. Two well established foundations are IIC [IIC] and OPC-UA [OPC]. For example, a [IIC_TALK] provided overview of IIC activities.

Industrial IoT Consortium (IIC) provides use cases, scenarios, and best-practice frameworks to solve specific problems and solution pain points. It is a rich resources of case studies and demonstrations of different test beds. The IIC itself is not involved in standards development, but may help in formalizing requirements, further insights into solutions developed in IETF, and potentially help adoption of those solutions.

Open Platform Communications-Unified Architecture (OPC-UA) provides interoperability across different hardware platforms using a standard data model. It standardizes various information models, corresponding client-server architecture and defines necessary access mechanisms to those information models. The OPC-UA is an abstraction layer to provide common interface to different data look-up and event notifications. A number of information models are provided by OPC-UA can be found here [OPC_INFO]. Foe example, OPC has a specification on PLCs. It abstracts PLC specific protocols (such as Modbus, Profibus, etc.) into a standardized interface allowing HMI/SCADA systems to interface with a middleware that

converts generic-OPC read/write requests into device-specific requests and vice-versa.

Note: OPC-UA information model similar to YANG?

IETF solutions will focus on leveraging or extending IETF technologies for IT and OT integration which is at the infrastructure or communication layer. Thus, providing protocols that could potentially benefit higher-level OPC-UA work.

Both IIC and OPC could provide guidance to the lower level work.

*For Discussion: assuming there is an IIN framework - how does it fit in the OPC-UA architecture and facilitate adoption of existing information models.

4. IIoT New Requirements

Traditionally, OT and IT experts have focussed on different concerns. On a production floor or with OT, the focus is generally on no-congestion, lossless reliable transmission, and real-time or deterministic communication. Quality of manufactured goods, and efficiency of processes is also an important concern for OT experts.

With Industry 4.0 initiatives (such as smart factory and smart manufacturing), these concerns are beginning to overlap, i.e. OT networks are also required to be concerned with scalability, security, operations and maintenance from remote locations.

The fundamental requirement for industrial networks is to support legacy devices (even when the network infrastructure is upgraded) while enabling emerging applications.

*Requirements from legacy device support:

1. Support for protocol formats and their core capabilities.
2. Support for traffic profiles for different types of services
3. Support for security and separation as designed in OT systems.

*Requirements from Emerging Trends:

1. Support device to cloud communication (remote operations)
2. Virtualization (virtual PLCs, digital twins)
3. High-volume data emission (analytics and surveillance)
4. Explicit location awareness (to determine edge networks, latency sensitive controls, safety operations).

5. Enhanced Industry data and device security (movement of sensitive data and remote control)

4.1. Device to Cloud Mechanisms

Perimeter of device control is expanding from factory floors to the cloud. It is anticipated that Industrial IoT controls when extended to the cloud or edge compute platforms will offer better integration with sophisticated business logic application architectures.

With adoption of virtualization several of supervisory or management equipment could transition to IT infrastructure. It may or may not remain on-premises. All scenarios are possible - moving L1,L2, L3 to separate IT network on the same floor, to the edge or to the cloud. Now extending the communication to the edge and cloud nodes increases the distance requiring adoption of layer 3 network designs.

4.2. Preserving Performance and Deterministic Behavior

Shorter addresses are inherent to industry control systems to provide implicit determinism. For this purpose, the industrial networks use fieldbus interface with the controllers.

4.3. Preserving Safety and Task outcomes

4.4. Interoperability with IP-world machines

To develop further on different type of address format support. From smaller address of legacy devices to IT based applications with IP address.

```
(OT-Address)--->(Industry Control)--->(IP-Address)
(control dev)       ( network )       (application)
```

Preferably allow OT devices to understand IP-addresses for the servers they connect to.

4.5. Digital Twin

Note: Should we include this. A digital twin is a virtual 3D representation of the real world. It can show physical objects, processes, relationships, and behaviors - and it can represent them as they are now, as they were in the past or will be in the years ahead. Some discussions have already begun, for example [I-D.draft-zhou-nmrg-digitaltwin-network-concepts].

5. IIN Framework

Above mentioned emerging trends such as virtualization of PLCs or moving MES or HMI into the cloud will have a significant impact on the framework. It moves functions from manufacturing zone to the cloud which not only influences how latency, safety and resiliency can be assured but also moves the security zones.

5.1. Distributed Architecture

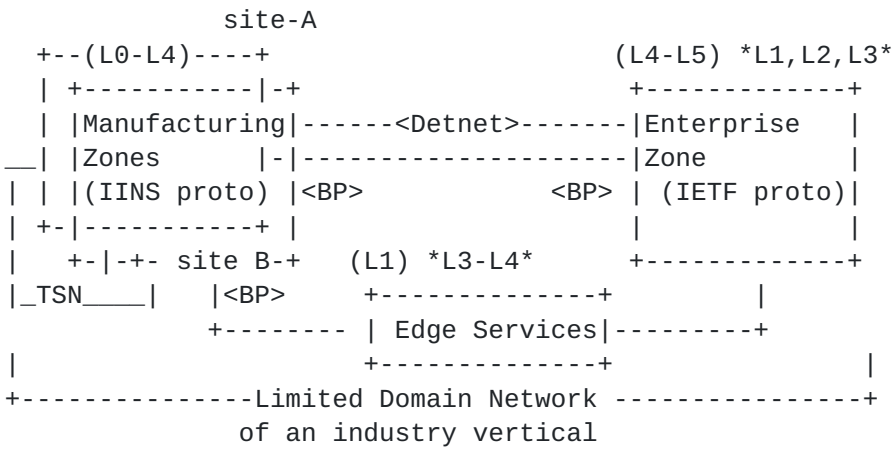

Figure 2: Integrated Framework with new placements for ISA 95 levels

In Figure 2, LDN taxonomy of internal, external and boundary protocols is used. The round brackets represent current Purdue model levels. Note that both Manufacturing and Enterprise zones are 'inside protocols' in LDN terminology but can (or may) run different protocol stacks. Each zone may deploy either custom of standard protocols. They interact using outside protocols i.e., public Internet technologies. The translation from inside to outside protocol happens through boundary protocols (shown as <BP> in the figure).

*__IINS (Integrated Industrial Network Stack) Protocols:__ A set of inside protocols that are used in traditional manufacturing zones. These are expected to support and extend existing industry protocols or may even be new extensions. Note that as a level component moves to cloud, those IINS will have to be supported in the cloud as well.

5.2. Interfaces

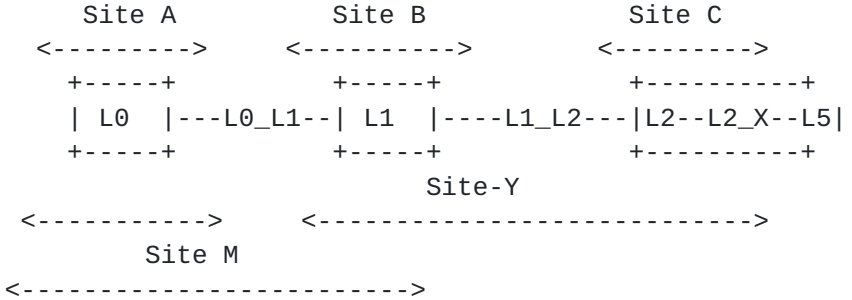

Figure 3: Interfaces dependent on the levels

Figure 3 above depicts that in IIN framework, boundaries between the interfaces should not be crossed. Moreover, equipment or functions

from different levels may be placed at different sites, but in this framework direct communication from higher levels to devices is not permitted.

*L0_L1 interface decides the communication channel between the process and basic control levels even when there may be a number network devices. These network devices are typically IIoT gateways that perform protocol translations (such as Modbus to Profibus).

*L1_L2 interface serves as communication between supervisory control devices and PLCs.

*L2_X interface is very likely IP interface for levels beyond L2, not sure if need to define an interface. it will be used for IT enterprise applications. however, it will still need to participate in functional requirements of data security and operational safety (meeting latency, resiliency targets).

Note: later add network device details in between.

Each interface has at least three attributes associated - whether a particular request is authorized, the service level guarantees (latency, data rate, frequency, etc), security profile.

In Figure 3, a level based hierarchical co-location is shown to be preserved.

*L0 is site A, L1 is site B and above L2 in site C.

*L0 is site A, L1 above in Site Y.

*L0, L1 in site M and above L2 in site C.

5.3. IIN Device Functions

These functions apply to end nodes as well as network nodes or other gateways in the network.

The topologies in the manufacturing zones do not change very frequently and devices are also designed for long-term use with minimal time between the failures. Such design considerations may be used to simply network operations and configurations.

Assuming this is a layer 3 network architecture, there should be an assignment and association between the network address and end devices' physical addresses. Note that legacy devices are either on serial bus or their information is carried over Ethernet media.

Further motivation and analysis for adapting to OT/IT asymmetric address formats is covered in [I-D.draft-km-industrial-internet-requirements].

Additionally, adapting these devices to network layer requires support for the following mechanisms:

5.3.1. Device Specific functions

*discovery and on-boarding

*Device identification and authentication

*Device addresses and their assignment and management

5.3.2. Transmission (Transport) Mechanisms

Currently, L0 and L1 devices do not use any transport protocol. The data is embedded after control header. With a network layer solution, TCP maybe too heavy for field-bus devices. Some other means of assuring device delivery will be needed.

5.3.3. Routing considerations to provide safety & security

Routing protocols will be necessary as the scale of the devices grow at the same time it should be kept simple. Possibly, Interior Gateway Protocol (IGP) will be deployed. Here it may be useful to provide guidelines on IGP features that provide distribution of routes (for different devices), path information.

5.3.4. Traffic Profiles for different type of data

Differentiating traffic and assigning priorities is required so that important data is not dropped. This is in addition to use of Detnet for time-sensitive services.

Different type of data can include - process data (high priority), monitoring data (low priority), fault, alarms, signals data (high), health-check sensors data (medium), etc.

Todo: Also discuss Detnet [DETNET] here.

6. IANA Considerations

This document requires no actions from IANA.

7. Security Considerations

This document introduces no new security issues.

8. Acknowledgements

9. Informative References

[DETNET] Finn, N., Thubert, P., Varga, B., and J. Farkas, "Deterministic Networking Architecture", RFC 8655, DOI 10.17487/RFC8655, October 2019, <https://www.rfc-editor.org/info/rfc8655>.

[I-D.draft-km-industrial-internet-requirements]
Makhijani, K. and L. Dong, "Requirements and Scenarios for Industry Internet Addressing", Work in Progress, Internet-Draft, draft-km-industrial-internet-requirements-00, 10 June 2021, <https://www.ietf.org/archive/id/draft-km-industrial-internet-requirements-00.txt>.

[I-D.draft-zhou-nmrg-digitaltwin-network-concepts]
Zhou, C., Yang, H., Duan, X., Lopez, D., Pastor, A., Wu, Q., Boucadair, M., and C. Jacquenet, "Digital Twin Network: Concepts and Reference Architecture", Work in Progress, Internet-Draft, draft-zhou-nmrg-digitaltwin-network-concepts-05, 25 October 2021, <https://www.ietf.org/archive/id/draft-zhou-nmrg-digitaltwin-network-concepts-05.txt>.

[IIC] "Industry IoT Consortium", n.d., <https://www.iiconsortium.org>.

[IIC_TALK] William Diab, W., "Overview of IIC – Building the IIoT Ecosystem", 12 October 2021, <https://github.com/iot-dir/Meetings/blob/main/20211012/slides/Diab_IIC_Overview_for_IETF_1021_rev2.pdf>.

[ISA95] "ANSI/ISA-95.00.01-2010 (IEC 62264-1 Mod) Enterprise-Control System Integration - Part 1: Models and Terminology", n.d., <https://www.isa.org/standards-and-publications/isa-standards/isa-standards-committees/isa95>.

[LDN] Carpenter, B. and B. Liu, "Limited Domains and Internet Protocols", RFC 8799, DOI 10.17487/RFC8799, July 2020, <https://www.rfc-editor.org/info/rfc8799>.

[OPC] "Open Platform Communications", n.d., <https://opcfoundation.org>.

[OPC_INFO] "OPC-UA Information Model Specifications", n.d., <https://opcfoundation.org/developer-tools/specifications-opc-ua-information-models>.

[SURV] Galloway, B. and G. Hancke, "Introduction to Industrial Control Networks", IEEE Communications Surveys & Tutorials Vol. 15, pp. 860-880, DOI 10.1109/surv.2012.071812.00124, 2013, <https://doi.org/10.1109/surv.2012.071812.00124>.

Authors' Addresses

Kiran Makhijani
Futurewei
Santa Clara, CA 95050,

United States of America

Email: kiran.ietf@gmail.com

Lijun Dong
Futurewei
Santa Clara, CA 95050,
United States of America

Email: lijun.dong@futurewei.com