Independent Submission
Internet-Draft
Intended status: Informational
Expires: December 12, 2021

K. Makhijani
L. Dong
Futurewei

June 10, 2021

Requirements and Scenarios for Industry Internet Addressing
draft-km-industrial-internet-requirements-00

Abstract

Industry Control Networks host a diverse set of non-internet protocols for different purposes. Even though they operate in a controlled environment, one end of industrial control applications run over internet technologies (IT) and another over operational technology (OT) protocols. This memo discusses the challenges and requirements relating to converegence of OT and IT networks. One particular problem in convergence is figuring out reachability between the these networks.

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 December 12, 2021.

Copyright Notice

Table of Contents

1. Introduction

An industry control network interconnects devices used to operate, control and monitor physical equipment in industrial environments. These networks are increasingly becoming complex as the emphasis on convergence of OT/IT grows to improve the automation. On one side of Industrial internet are the inventory management, supply chain and simulation software and the other side are the control devices

operating on machines. Operational Technologies (OT) networks are more often tied to set of non-internet protocols such as Modbus, Profibus, CANbus, Profinet, etc. There are more than 100 different protocols each with it's own packet format and are used in the industry.

It is expected that integration between the IT and OT will provide numerous benefits in terms of improved productivity, efficiency of operations by providing end to end visibility and control. Industry control applications also expect to operate at cloud scale by virtualization of several modules (especially PLCs) leading to new set of network requirements.

One aspect of industry control is the delivery of data associated with the Real-time, deterministic and reliability characteristics over local-area and wide-area networks. This type of inter-operability functionality and study is already covered in DETNET working group. The other aspect is rachability and interconnection keeping heterogenity of communication interfaces and a variety of services in mind. This doument focuses on the latter part only.

OT networks have been traditionally separate from the IT networks. It allowed OT network experts to manage and control proceses without much dependency on changes in the external networks. This is an important to consideration when dealing with the industry control networks to maintain them in a controlled environment leveraging the limited-domain networks [LDN] concept for an independent network control.

The purpose of this document is to discuss the reachability and interconnection characteristics, challenges and new requirements emerging from large-scale integration of IT and OT.

2. Terminology

- Industrial Control Networks: The indutrial 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 fieldbus devices, digital controllers and software applications

- Industry Automation: Mechansims 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.

- Human Machine Interface: An interface between the operator and the machine. The communication interface relays I/O data back and

forth between an oeprator's terminal anf HMI software to control and monitor equipment.

2.1. Acronymns

- HMI: Human Machine Interface

3. Industrial Network Reference Architecture

In the scope of this document the following reference industrial network will be used to provide structure to the discussion. In the Fig. Figure 1 below, a hierarchy of communications is shown. At the lowest level, PLCs operate and control field devices; above that Human Machine Interface (HMI) interconnects with different PLCs to program and control underlying field devices. HMI itself, sends data up to applications for consumption in that industry vertical.

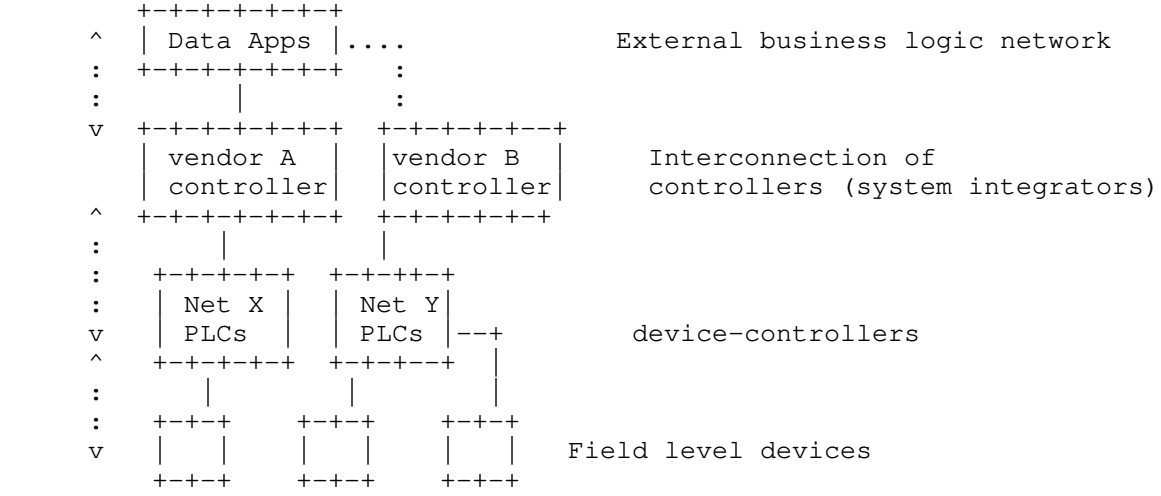


Figure 1: Hierarchy of Functions Industrial Control Networks

Unlike commercial networks that uniformly run IP protocols, the communication links run different protocols at along the different level of the hierarchy. One of the key requirement from new industrial applications is the integration of different types of communication protocols including Modbus, Profinet, Profibus, ControlNet, CANOpen etc.

A vertically integration system involves a network between the external business applications and higher controllers (for e.g. SCADA, HMI, or system integrators) is IP based. The second level of networks between the controllers can be either IP or non-IP

(Profibus, BACNet, etc.). The lowest field-level networks between industrial controllers and field-level may be any of the fieldbus or device control protocols (More details of the industry networks can be found in [SURV]).

3.1. Communication Patterns

The following communication patterns are commonly observed:

- controller to controller: A communication between multi-vendor controller maybe required by system integrators to work in complex systems.

- controller to field level devices: This is a fieldbus communication between device such as I/O modules, motors, controllers. This communication represent.

- Device to device: allows direct communication between wired industrial devices and wireless devices to enhance automation use cases. For an exmaple, use of camera to visually monitor and detect anamolies in other devices.

- controller to compute: vertical communication between a controller and compute integrates IP-based technologies with non-IP since OT product systems and solutions are not connected with IP based networks.

A certain level of inter-operability is required to exchange data between the above endpoints from different vendors. One of the challange is that Ethernet (which unifies IT standards) that's not always possible in Industry networks.

3.2. Industry Control Network Nuances (current state)

The Industry control networks are engineered for the idustry verticals they belong to and depict unique properties as below:

- location bound: The Control Device's location or the network they are attached to is predetermined and changes rarely. However, the network resources may not get efficiently utilized to avoid contention between them.

- security by separation: Typically, security is enhanced by keeping IT/OTnetworks separate. The operators control how data goes in and out of a site through firewalls and policies.

- data growth: Even though the size of network remains the same, data generated is much higher. For example, cameras installed for

visual inspection to determine the quality of manufactured product generates a high bandwidth demand.

- Wired device constraints: A bulk of machines are over wired network, their constraints vary from LPWAN and IoT devices which is an active area of standardization work. device lifetime, or power-requirements are not typical constraints. Instead direct process control mechanisms are more important.

- Real-time behavior: The control devices require realtime as well as deterministic behavior between a controller (such as an HMI station) to the equipment. The DetNet working group covers several aspects.

The goal of the document is not to reinvent the Industry control infrastructure. See section Section 6 on related standards work. It is meant to exclude the already covered by other WGs.

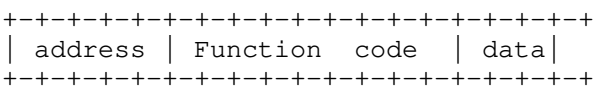
Since a device connects to network through its address, the document explores different address specific nuances in control devies - such as management, device discovery and integration requirements. This document concerns with the identification of and role networks, specifically from the organization of industry control devices.

The goal of this document is to outline some of the challenges and improvement of connectivity aspects of Industry control networks.

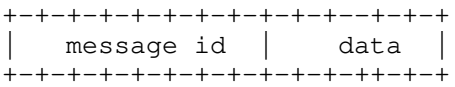
4. Problem Statement

In industrial networks, a good number of devices still communicate over a serial or field bus (although Ethernet is being gradually adopted). The operations on these devices are performed by writing provide direct access to operation-control. i.e what operation to perform is embedded in the type of interface itself. For instance, Profibus, Modbus networks are implicitly latency sensitive and short control-command based.

ModBus



CANBus



Profibus - todo.

Since they are localized in an area such as factory floor or a site, such networks have evolved independently and are seperated from the IT applications. The emerging trend requires a seamless integration with intelligent software, sophisticated compute platforms and other operational aspects as highlighted below:

4.1. Heterogenity

A typical industry control network has devices of different communication interfaces such as Fieldbus (PROFIBUS, Modbus, and HART), Ethernet (generic Ethernet/IP, PROFINET, and Modbus-TCP), and also wireless (Bluetooth, Wireless HART, and IoT). These interfaces vary at the physical and link layers and because they integrate with their own application technologies providing interoperability between these devices remains a challenge. This also makes difficult to adopt to modern integration technologies.

Fieldbus client-server architecture is widely deployed. It delivers commands deterministically from a controller to the device and vice-a-versa. Interfaces of this kind have typically shorter addresses (upto 256 devices on a single bus in Modbus).

Some of the servers also behave as protocol gateways and interconnect different type of protocols. For example when a modbus device is being controlled by a profinet server, an gateway function will translate modbus data or encapsulate it over IP (if the controller supports it).

In a Gateway-centric approach, gateways are in charge of protocol translations between the devices with different interfaces. This requires packing and unpacking of data in the source and destination formats at the attached gateways. Note: As an example, a Modbus device does not know whether to send command to Profibus PLC or Modbus PLC. The gateway device attaches to performs the translation. This is even worse with encapsulations, where the entire frame is carried over IP.

This is not ideal for latency sensitive applications. Although hardware wise, gateways need to be equipped with all the interface, it is more efficient to only perform data link conversion.

4.2. Automation Impact

Automation of processes in industry relies on control sophisticated technologies such as machine learning, big data, etc. with minimal human intervention. Automation needs to support scale, reliability and resiliance at large-scale.

4.2.1. Scale

Automation control at small scale applications with well defined task has been possible. In order to improve production, and eliminate stoppages and minimizing human intervention.

When the number or density of devices, and processes increase there is a need to schedule, route, and coordinate over multiple control environments.

4.2.2. Stretch Control Fabric to Edge and Cloud

The industry control networks can be extended to cloud or edge compute platforms. Since these networks are not equipped with compute intensive servers. Now extending the communication to the edge and cloud nodes increases the distance requiring traditional L2 networks to be adopted to L3 network designs.

Design decisions will require to choose different transit strategies (this maybe layer 1, 2, 3 technologies or even network slices). It also influence the security policies.

4.2.3. Reliability

Production efficiency is inversely related to number of defects in a process. System reliability is determined through measurements of its instantaneous state.

Automation processes need to ensure that system is performing in an expected state and is capable of reporting anamolies fast and accurately (i.e. packet drops or jitter leading to poor quality product).

4.2.4. Resilience

TBD.

4.3. OT/IT Convergence

Most of the factory floors are not equipped with IT servers to perform compute intensive tasks. Yet an IP-based device need to connect with non-IP interface to control those devices.

Often real-time response is necessary for example, in closed-loop control systems direct communication is desired to avoid any additional packet processing delay or overheades at the source and destination gateways, equipping IP to all OT devices and abandoning

the existing investment and depolyment could result in the following obvious problems.

- Many of the standard IP based protocols maybe too much overhead for OT devices.
- Cannot preserve communication characteristics of devices (different device addressing scheme, realtime, IRT, message identifiers, Bus-like properties).
- It relies heavily on hierarchy network stack (network layer, transport layer, application), where as OT devices do not have any, they generally operate at data link layer or below.

4.4. Data oriented networking

Industry verticals keep data and control on the manufacturing floor, on a closed system. There is no easy way to forward this data to enterprise level software. On premise micro data centers or edge computing are new infrastructure pieces that wil impact the design of current industrial networks.

4.5. Virtualization

Traditional Industry control infrastructure is not virtualized. Virtualization will enable deployment of new functionality in a flexible manner.

- Virtual PLCs are considered an important component functionality customization of digital-twin realization.
- virtualization enables edge and cloud native computing by moving and instantiating workflows at different locations.

Implications that PLCs are no longer one-hop away.

5. Address Space Requirements

5.1. Short Device Addressing

Shorter addresses are inherent to industry control systems to provide implicit determinism.

Note: The motivation for short address is to preseve the legacy attributes of fieldbus control devices. It is not related low-power or resource constraints.

A large volume of the messages are of sizes shorter than the size of IP headers (v4, v6) themselves. The header tax will be very high over industry control networks.

5.2. Meaningful Addresses

The industry control floors are built bottom-up. The devices are carefully wired and connected to controllers. In a hierarchical network design, a particular type of machine can be reached in a structured manner by adding subnet or location to the address structures.

5.3. Device name based Addresses

HMI might require human readable address that is undertandable to human operators or application end users. For example, a device address could be associated with its location, type of applications, attached objects etc. The network needs to support the resolution and routing based on such device addresses, which is more user friendly. On the other hand, grouping devices based on their addresses shall be easily implemented to enable group operation and communication.

5.4. Adoption of Lean Network Layer

Challenge of Industrial network device address is that it communicates to a physical device address. Traditionally, in a limited environment there was no need for network layer or expressing network specific service, access control.

- If a sensor is broken, it will require reprogramming of controller and re-aligning with the new address. The benefit of network layer, removes this restriction.

- Note that, using IP stack is not suitable because these devices perform specific functions and any overhead in transport or large addressing can add to processing delays.

- Several other IP suite protocols such as device discovery should be revisited.

5.5. Multi-semantic behavior

OT networks, at least at site level are organized at much smaller scale than typical IP-capable networks. There is in turn a fixed hierarchy of networks w.r.t. location in a plant.

5.6. 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.

6. Relationship with Activities in IETF

6.1. Deterministic Networks (DetNet WG)

The Deterministic Networking (DetNet) [DETNET-ARCH] is working on using IP for long-range connectivity with bounded latency in industry control networks . Its data plane [DETNET-DP] takes care of forwarding aspects and most close to Industry control networks but the focus is on the controlled latency, low packet loss & delay variation, and high reliability functions. Not dealing with interconnection of devices.

In layer 2 domain, similar functionalty is convered by TSN Ethernet [IEEE802.1TSNTG].

6.2. IoT OPS

IoT operations group discusses device security, privacy, and bootstrapping and device onboarding concepts. Among the device provisioning one of the object is network identifier. We understand that the IoT OPs does not exclude evaluation of industry IoT or control devices requirements. Given the specific functions described above it maybe necessary to configure more than an identifier, i.e. server or controller information or specific address scope and structure.

6.3. LPWAN

The LPWAN has focussed on low-power and constrained devices. There are compression related approaches that may apply are [SCHC] or [ROHC]. To be evaluated for process control devices.

6.4. Recent Addressing related work

Some of the work initiated on the addressing include solutions such as [FlexIP], [Flexible_IP], [FHE], and [SOIP].

Recently, a broader area of problem statement and challenges in [CHALLEN].

7. IANA Considerations

This document requires no actions from IANA.

8. Security Considerations

This document introduces no new security issues.

9. Acknowledgements

10. Informative References

[CHALLEN] Jia, Y., Trossen, D., Iannone, L., 3rd, D. E. E., and P. Liu, "Challenging Scenarios and Problems in Internet Addressing", draft-jia-intarea-scenarios-problems-addressing-00 (work in progress), February 2021.

[DETNET-ARCH] 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>.

[DETNET-DP] Varga, B., Ed., Farkas, J., Berger, L., Fedyk, D., and S. Bryant, "Deterministic Networking (DetNet) Data Plane: IP", RFC 8939, DOI 10.17487/RFC8939, November 2020, <https://www.rfc-editor.org/info/rfc8939>.

[FHE] Jiang, S., Li, G., and B. Carpenter, "Asymmetric IPv6 for Resource-constrained IoT Networks", draft-jiang-asymmetric-ipv6-04 (work in progress), November 2020.

[Flexible_IP] Jia, Y., Chen, Z., and S. Jiang, "Flexible IP: An Adaptable IP Address Structure", draft-jia-flex-ip-address-structure-00 (work in progress), October 2020.

[FlexIP] Moskowitz, R., Li, G., and S. Ren, "FlexIP Addressing", draft-moskowitz-flexip-addressing-00 (work in progress), January 2019.

[IEEE802.1TSNTG] "IEEE, "Time-Sensitive Networking (TSN) Task Group"", 2018, <https://1.ieee802.org/tsn>.

[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>.

[ROHC] Jonsson, L-E., Pelletier, G., and K. Sandlund, "The RObust Header Compression (ROHC) Framework", RFC 4995, DOI 10.17487/RFC4995, July 2007, <https://www.rfc-editor.org/info/rfc4995>.

[SCHC] Minaburo, A., Toutain, L., Gomez, C., Barthel, D., and JC. Zuniga, "SCHC: Generic Framework for Static Context Header Compression and Fragmentation", RFC 8724, DOI 10.17487/RFC8724, April 2020, <https://www.rfc-editor.org/info/rfc8724>.

[SOIP] Carpenter, B., Jiang, S., and G. Li, "Service Oriented Internet Protocol", draft-jiang-service-oriented-ip-03 (work in progress), May 2020.

[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.

Authors' Addresses

Kiran Makhijani
Futurewei

Email: kiran.ietf@gmail.com

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

Email: lijun.dong@futurewei.com