Internet Area Working Group
Internet-Draft
Intended status: Informational
Expires: 8 January 2023

C. Westphal
K. Makhijani
Futurewei, USA
K. Dev
Munster Technological University, Ireland
L. Foschini
University of Bologna, Italy

7 July 2022

OCN Use Cases for Industry control Networks
draft-wmdf-ocn-use-cases-00

Abstract

This document present industrial networking use cases for Operations and Control Networks (OCN). It is a companion document to the OCN reference model and the OCN problem statement and requirements document. This document compiles a list of potential use cases where new industrial networking protocols could be beneficial.

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

This document present the OCN Industrial Use Cases. OCN stands for Operations and Control Networks. It is believed that current network protocols are not flexible enough to allow deployment in industrial networks.

Industrial networks have a specific set of requirements and existing solutions and technologies. It is however expected that the deployment of 5G and of solutions to extend the WAN into distributed and potentially remote or hard to reach locations would dramatically alter the way these networks are deployed, managed and operated.

In particular, it is expected that these networks would interconnect a wider range of networks potentially at a global scale; would interface and peer with a wider number of potential networks, including the global Internet; and would coalesce around a unified set of protocols, both to commoditize and reduce the cost of the industrial network infrastructure, and to offer interconnection with a wider set of networks over these unified protocols.

In this document, we first give a quick background on OCN and industrial networks, and then present use cases where new industrial network protocols would potentially bring new features and new services.

These use cases could potentially be solved with current technology, or are active areas of investigation. However we believe that eventually, some unified set of protocols would be useful that supports these use cases. While we make no proposal for such protocol, we believe it would be of value to the community to seek to design such protocols.

2. Conventions and Definitions

We provide some definitions and acronyms that are relevant to this document:

Industrial Control Network: Industrial control networks are the interconnection of equipment used to operate, control, or monitor machines in the industry environment. It involves different levels of communications between field bus devices, digital controllers, and software applications.

Industry Automation: Mechanisms that enable the 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: Control loops are part of process control systems in with desired process response is provided as an input to the controller, which performs the corresponding action (using actuators) and reads the output values. Since no error correction is performed, these are called open control loops.

Feedback Control Loop: Feedback control loop is a system in which the output of a control system is continuously measured and compared to the input reference value. The controller uses any deviation from the input value to adjust the output value for the desired response. Since there is a feedback of error signal to the input, these are called closed control loops.

Programmable logic controllers (PLC): Industrial computers/servers to control 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.

Fieldbus Devices: A device which is installed on the field (e.g., solar farm, energy grid, autonomous vehicle). Operational Technology field devices include valves, transmitters, switches, actuators, etc.

Operations and Control Networks (OCN): A network that supports all the capabilities necessary to accomplish a process or control command execution on actuators for the desired effect prescribed by the controllers based on continuous inputs from the sensory data and application requests.

3. Background and Framework

Traditional communication networks facilitate the data communication between multiple devices and peripherals. With the evolution of devices and systems such as Internet of Things (IoT) and cyber-physical system (CPS), the characteristics of a network has undergone great changes. In order to accommodate IoT and CPS, Industrial Communication Networks were introduced that could handle data integrity and real-time control for large installations in harsh environments. The purpose of these networks is to connect sensors (devices that monitor some parameter at a site), actuators (devices that perform an action in the physical world), controllers and other elements that require some specific network services.

In Industrial applications, these networks include ControlNet, Modbus, DeviceNet, Ethernet, Profinet and so on. They form a connection among PCs, controllers, and field devices which is difficult to do with traditional communication networks.

Industrial Ethernet is used extensively which is part of industrial automation, but with the advent of 5G and mMTC, it is expected that industrial networks would expand to a global reach. This creates new constraints to meet the real-time operational needs. These networks to support increasingly large number of devices with a wide range of standards and policies. Furthermore, the factory system should offer solutions with great reliability, efficiency, and fast or even deterministic response times.

The OCN problem statement we consider stems from [OCN-PS].

We consider here industrial systems and networks, and they have a wide range of applications. As a consequence, they operate in a wide range of conditions as well, which poses a challenge to operate and manage these networks. The level of required connectivity will vary between devices within a network, and between the applications of the

network within an industry. A manufacturing plant may have remotely controlled robots that perform assembly of a product, which have a much lower latency requirement than, say, a solar farm.

For Industry control systems, there are different types of end-points and different types of traffic in between. Some data traffic essentially convey instructions that need to be delivered within a specific time to perform a task at a machine or equipment. Some may have more elastic latency requirements. Some interactions between two end-points may be atomic, while some may require to convey some contect, or to maintain some state either within the network or at one or both of the end-points.

The end-points in such systems can be either a controlling entity, sensors or actuators. Sensors and actuators are assumed to not perform decision making tasks. The controller has those responsibilities.

The packets delivered from the controller are the actionable instructions to actuating device. They may fit into a single packet, or be part of a data stream. Many IoT application would have smaller packets, and therefore require consideration of packet overhead.

Some other applications may require stream, for instance in case of videosurveillance of industrial operations.

We briefly recall the main components of the OCN framework (for more details, see [OCN-RM]).

An OCN is a network used to connect three basic types of functional devices - actuators, sensors and controllers. They are well-known in the industry control systems (ICS) and are generalized to include all kinds of OCN scenarios. The sensors and the actuators are associated with physical, logical, or digital entities that can be observed, monitored, or caused to move or change. An OCN connects field devices, with the controllers and associates them for the exchange of data to trigger and monitor changes to achieve desired effect.

The OCN connects these elements to support the services that enable the deployment of an industrial network, including providing some guarantees for certain type of services, some reliability, or some security. Indeed, an industrial application may have strict latency requirements, for instance to control remotely the operation of some machinery. It may also have some reliability requirement, as any down time may impact the bottom line of the industrial application it supports; and it should be robust to some attempts to disrupt the production from adversary entities. Privacy may be a requirement as well.

The OCN framework is not limited to industrial networks. Smart Grid or Self-Driving Cars for instance could be areas of application. Any network that supports sensors, actuators and controllers is a target for deployment of such network. We focus here on the use cases in the industrial/manufacturing sector, as it is expected that most machine-to-machine deployments would occur in the near future.

4. Industrial Use Cases

This section lists some of the Use Cases we anticipate for OCN. This list is not exhaustive, and some of the use cases may be supported using current technologies. We believe however that the superset of these use cases would provide basis for establishing a set of requirements for OCNs in the future. This list is open for discussion.

4.1. Protocol Convergence

Currently, a hodgepodge of protocols are used in Industrial networks. We mentioned ControlNet, Modbus, DeviceNet, Ethernet, Profinet above. It is detrimental to the industry to have many protocols that cannot easily interoperate and have different support for different services.

To reach a critical mass and to decrease the unitary cost of a device through economies of scale, we believe there is a need to unify these protocols into one common protocol. We need a glue to connect these different networks together, similary to the way that the Internet became successful once a common narrow waist was defined and provided.

One special case is that of the field bus convergence protocol. Field bus are typically serial devices with limited range.

A complex automated industrial system has typically a hierarchical structure, denoted distributed control system (DCS). The top of the hierarchy for production management is connected to a control level of Programmable Logic Controllers (PLCs). This is typically done via Ethernet. The Fieldbus then links the PLCs to the control level of the components, namely sensors, actuators, switches, etc. The fieldbus is therefore time-critical. Fieldbuses are currently deployed over Industrial Ethernet, that is the use of Ethernet in an industrial environment that supports determinism and real-time control.

Protocols for Industrial Ethernet include EtherCAT, EtherNet/IP, PROFINET, POWERLINK, SERCOS III, CC-Link IE, Modbus TCP, CANopen, MQQT, etc. Most of these protocols are at layer 2. Translating

protocols to interoperate as well as to extend the range beyond the LAN would require new layer 3 protocols to connect the sensors, actuators and controllers in a more universal manner.

In the OCN reference model, this use case connects sensor points (SPs), actuation points (APs) and controller points (CPs) using a unified OCN communication interface, to support delivery of OCN message of multiple types (in-time, on-time, bounded latency, periodic, etc.) as required by the underlying protocol that the OCN is emulating and/or replacing.

4.2. Self-Configuration of Industrial Networks

Adding new device in a distributed network, where the facilities have a large footprint, needs to be supported in the OCN. Bootstrapping is a significant use case for a network that orchestrate and coordinates between a large number of sensors, actuators and controllers.

Further, an OCN is a potentially large collection of devices that may be constrained in some way. This means that the configuration of new field devices needs to be done in a scalable manner yet without burdening the devices with too many omputational steps (say, crypto computations), large exchange of data (say, firmware uploads) or other similar considerations.

The deployment of such a network requires that the devices may be added to the network in a simple model, or removed from the network, or updated or modified, in a scalable manner.

The OCN protocol need to support some form of authentication for new devices, or to have the ability to filter the data from devices (including field devices) so as to remove unwanted packets or to refuse transmission of data from unknown devices. The data from the devices can be equipped with some authentication tokens or certificates that can be verified in the OCN.

Some of this use case may be covered in the IETF IoTOPS, that deals with networked devices with a limited user interface and deployed in large numbers. This could apply to some controllers, actuators and sensors in an OCN. However, the indutrial networks have specific requirements to be considered here.

This pertains to the bootstrapping of an OCN, where the number of

Actuation Points (APs), Sensor Points (SPs) and controller points (CPs) is potentially large and cannot be configured manually. Some of the message types to be supported include asynchronous messages and periodic message for pushing firmware updates or checking the liveliness of a field device (AP, SP or CP).

4.3. 5G Private Networks

One key aspect of 5G is to enable massive machine-to-machine (massive Machine-Type Communication - mMTC) over 5G private network or 5G campus networks. This allows a large number of devices in distributed domains to connect together into a single industrial network.

Private network can connect devices that could not be reached beforehand with a combination of wireless connectivity, WAN connectivity, and cloud connectivity.

This allows to connecting devices at a much larger scale than current wifi deployments, for instance. In the extreme, the whole industrial network could be connected into one single network domain where all the devices are reachable.

Once consequence of a uniform network deployment would be to deploy networks - and devices within that network- using a single standard technology, rather than every industry creating their own idiosyncratic solution.

The OCN interface in this use case has a much larger footprint, which requires care to support certain types of OCN messages (in particular in-time or bounded latency messages) due to the potential physical distance between the CP and the APs/SPs.

4.4. IIoT

One specific case of industrial OCN is that of connecting IoT devices. The sensors and to some extent, the actuators, may have limited networking capability, due to for instance power constraints (due to battery-powered, or solar power devices).

Constrained devices in an industrial OCN require specific considerations. If the bandwidth of the link that connect to the devices is limited, the OCN protocol to exchange data should be designed carefully to minimize the overhead tax of the protocols.

Minimizing the protocol overhead may require to use flexible addressing scheme so that devices in a bandwidth constrained environment use shorter addresses than devices with plenty of bandwidth available. Similarly, devices that transmit small amount of data should also be careful to not use very long pacekt headers. Of course, such addressing scheme still needs to provide some reachability throughout the OCN domain, and potentially globally. The protocol overhead in OCN should be such that it operates in an efficient regime.

The OCN communication interface should therefore take into account the limits and constraints of the APs and SPs.

4.5. Large Volume Application

The opposite side of the coin of the previous use case is that of industrial networks that carry extremely large volume of applications.

For instance, some processes may require to extract a lot of information for continuous quality control. This could be composed of some data from sensors, some measurement data, some video stream extracted from a monitoring camera where product defects can be identified using image processing.

Other use case that generate large volume application would be the creation of a virtual environment that replicate off-site the conditions of the industrial facility, so that an operator can observe - or even participate within - that environment. Such an AR/VR use case would require a large amount of data to be transmitted from the industrial facility to the location of the operator.

Many pieces of equipment in an industrial environment also require continuous telemetry to monitor the functioning of the industrial facility, and potentially to identify conditions that may lead to failure ahead of time. This also requires the transmition of a continuos stream of data that could encompass many different dimensions, as well as the data processing functions to identify the signature of a potential failure (or whatever other use is applied to this data).

OCN therefore may require to transmit large amount of volumetric data. Techniques to support the transmission of large volume of data (in particular, proper transport protocols) are required to support this use case.

4.6. Remote Control

More and more industrial applications rely on controlling machinery from afar. Among the reasons for this use is to consolidate the control of several facilities into one location; to control facilities that are in hazardous or sterile environment. For instance oil extraction, refineries, mining industries are highly dangerous industries.

We envision the deployment of networks for the remote control of the equipment in such environment to ensure safer procedures. Remote control tools and robots can conduct the tasks that are risky for human beings. The OCN network to support this use case would need to meet some stringent availability requirements, as well as some latency (corresponding to the eventual industrial application).

Remote control is also a use case for vehicular network and remote driving, described in [OCN-remote-driving].

With respect to the reference model, this entails support of bounded latency, in-time, on-time message types as well as support of reliability requirements on the OCN network itself.

4.7. Determinism

Industrial applications often have requirements that cannot be provided by best-effort networks. As a result, some specialized protocols have been designed to provide performance guarantees beyond best-effort (BE).

IEEE 802.1 Time-Sensitive Networking (TSN) builds on top of Ethernet to provide reserved shares of bandwidth in a sub-network. However, there is a need to extend beyond Ethernet and still provide these same stringent guarantees across wider interconnected domains. [DetNet-TSN] extend this service to DetNet IP domains.

For the case of IIoT, [I-D.irtf-coinrg-use-cases] suggests leveraging in-network computation. The idea is that by bringing computation closer to the end devices, more stringent delay requirements can be achieved. However, this requires re-architecting the network to support computations within the network.

OCN requires stringent time constraints in many industrial applications. The operations of an actuator need to be executed with fine grained time accuracy. The OCN may extend beyond a domain of limited scope. THe controller may be in a different site, for practical or for safety reasons, or due to virtualization objectives (see the vPLC use case for instance).

In the reference model, this is captured by the in-time, on-time and bounded latency message types to be supported by an OCN.

4.8. Industry 5.0

Industry 5.0 is defined as the next phase of industrial production, after Industry 1.0 (the Industrial revolution of the 1800s with steam power), 2.0 (the adoption of electricy and of division of labor in the early 1900s), 3.0 (the appearance of electronics in production environment in the 1970s), 4.0 (smart manufacturing, in the 2000s). Industry 5.0 supports mass personalization of the production output. In this framework, collaborative robots (cobots) also communicate with humans to enable personalizable autonomous manufacturing.

To achieve this, the production requires to be integrated with variations from product to product. These changes need to be shared with the production line so as to integrate them within the product. The production line is the actuator, the controllers store the specificity of each produced item (say, a medical device that is specific to its user) and each specifications need to be shared across the OCN to each of the steps of the production line.

This use case requires APs to be dynamically configured and potentially updated between producing consecutive items, and support for bounded-latency message type would reduce the downtime and increase the productivity of the Industry 5.0 production facility.

4.9. Virtual PLC

Many current industrial applications run over Programmable Logic Controlers (PLCs). These are the basic building blocks of automation, and control sensors and actuators on factory floors.

PLCs are everywhere, and perform trasks such as motion control for robots, or smart manufacturing automoation.

There is a wide range of traditional PLCs, depending on size, type and function. Size range from nano (with less than 15 I/O points) to large (with over 512 I/O). As automation grows and becomes more dynamic, factory floors will need more and more PLCs with better performance, more flexibility and more I/Os.

For this purpose, it is suggested to virtualize the PLCs and to leverage the benefits (in terms of elasticity and scale) of virtualization for PLCs.

[PLC] defines virtualized PLCs as follows: "Virtualized PLC is a hardware-agnostic abstraction of the control unit and memory functions of a PLC. It is hardware- independent and still needs an interface to communicate with the I/O modules."

There are related trends to virtualized PLCs, such as the virtualization of HMI, SCADA MES, and other OT equipment, with the purpose of using general purpose hardware in a scalable manner; and to integrate higher lever functions that require more processing power.

The benefits of virtual PLCs are many: it allows to leverage more sophisticated compute and storage and virtualization technologies. It integrates multiple PLCs operations on one platform, removing some superfulous movement of data; it allows for tighter application integration; it allows to leverage better edge support; and it frees up some physical space on the factory floor as the control units could be remote.

Some instantiation of virtual PLC would require bettern network support. The virtual PLC can be separated from the hardware, using some abstracted interface. The Control Unit can be then placed across an OCN network, provided that it supports this placement away from the actuator.

The network needs to preserve the zone security and safety of operations, and to support timeliness of the delivery as required by the application of the PLC (the control unit and its related actuator).

For this use case, the network would provide a common interface between the device and the vPLC, as well as a unified converged fabric for all types of end-point. The OCN between the vPLC and the APs/SPs needs to support in-time, on-time, periodic, synchronous message types.

4.10. Simplification of OT/IT Integration

Industrial networks have multiple devices in a specific location, where changes are relatively rare. Many of them are wired devices from a network point of view, where direct process control loops are the more important aspect.

Security is often achieved by separation, and in particular by separating the OT infrastructure from the IT. The control loops oftern require deterministic network behavior.

This creates some challenges, in particular to deal with the heterogeneity of industry protocols. There are more than 100 protocols, where the controller sits behind one protocol and control devices; stateful gateways are often required to translate in between protocols.

This also hinders automation: the network is "engineered" to support a set of devices, and makes changes in the scale challenging.

One use case of OCN would be to simplify the integration of OT and IT and to allow to run industrial (process control) technologies over IP.

There are structural differences in addressing between IP and industrial protocols. IP offers a fixed number of bytes that identify a node. Industrial protocols in different process control zones have different address spaces. They typically don't have a network layer, but are scoped within a LAN. Protocol format conversions are possible and may happen on the fly: devices of one protocol often connect to controller of other protocols.

To enable a unified and simplied industrial network, we would need a comon network format that is friendly to both OT and IT applications. This needs to take into account that typical actuator and sensor data is often small, and could require either header compression or a flexible address structure.

A network layer would need to be defined, especially as it pertains to extending this use case to support virtualization of the controllers (vPLC, as in the previous use case).

4.11. Smart Contract

Devices in an OCN may need to support some operations that are specified by the controller under the form of a smart contract. For instance, some tasks may need to be specified by the controller as a function to be deployed in the field devices under the proper contract terms.

The OCN needs to support mechanisms to propagate such smart contract (which may be programs or instruction sets, or just some authenticated information to share between the devices) and to validate them throughout the OCN network.

This may relate to the configuration use case as well, since the contract may be to set up the device, for instance by specifying the credentials required for authentication and trust, and by setting up what type of function it will support.

Smart contracts may require as well some abstractions to be validated, either within the OCN or at the edge of the OCN, and either in a distributed manner or within a specified control point.

5. Security Considerations

OCN may have security implications to discuss in subsequent documents.

6. IANA Considerations

This document has no IANA actions.

7. References

7.1. Normative References

[I-D.irtf-coinrg-use-cases]
Kunze, I., Wehrle, K., Trossen, D., Montpetit, M., Foy, X. D., Griffin, D., and M. Rio, "Use Cases for In-Network Computing", Work in Progress, Internet-Draft, draft-irtf-coinrg-use-cases-02, 7 March 2022, <https://datatracker.ietf.org/doc/html/draft-irtf-coinrg-use-cases-02>.

7.2. Informative References

[DetNet-TSN]
Varga, B., Farkas, J., Malis, A., and S. Bryant, "Deterministic Networking (DetNet) Data Plane: IP over IEEE 802.1 Time-Sensitive Networking (TSN)", RFC 9023, 8 June 2021, <https://www.rfc-editor.org/rfc/rfc9023>.

[OCN-PS] "Problem Statement and Requirements for the Operation and Control Networks (OCNs)", n.d., <https://github.com/tabz11/IETF-OCN-1/blob/gh-pages/draft-tf-ocn-ps.txt>.

[OCN-remote-driving]
Dong, L., Li, R., and J. Hong, "Use Case of Remote Driving and its Network Requirements", Work in Progress, Internet-Draft, draft-dong-remote-driving-usecase-00, 27 June 2022, <https://datatracker.ietf.org/doc/html/draft-dong-remote-driving-usecase-00>.

[OCN-RM] "Operations and Control Networks - Reference Model and Taxonomy", n.d., <https://kiranmak.github.io/draft-kmak-ocn/draft-km-intarea-ocn.html>.

[PLC] Makhijani, K. and L. Dong, "Virtualization of PLC in Industrial Networks - Problem Statement", Work in Progress, Internet-Draft, draft-km-iotops-iiot-frwk-02, 5 March 2022, <https://datatracker.ietf.org/doc/html/draft-

km-iotops-iiot-frwk-02>.

Acknowledgments

TODO acknowledge.

Authors' Addresses

Cedric Westphal
Futurewei, USA
Email: cedric.westphal@futurewei.com

Kiran Makhijani
Futurewei, USA
Email: kiran.ietf@gmail.com

Kapal Dev
Munster Technological University, Ireland
Email: kapal.dev@ieee.org

Luca Foschini
University of Bologna, Italy
Email: Luca.Foschini@unibo.it