Workgroup: Internet Area Working Group
Internet-Draft: draft-km-intarea-ocn-00
Published: 2 July 2022
Intended Status: Informational
Expires: 3 January 2023
Authors: K. Makhijani   T. Faisal   R. Li
Futurewei   King’s College London   Futurewei

Operations and Control Networks - Reference Model and Taxonomy

Abstract

This text formulates a specialized network concept to support communication constraints in automated systems. These specialized networks, formulated as Operations and Control networks (OCN), are significant to many application scenarios involving the control and monitoring of mechanical and digital devices. The document defines the OCN reference model, describing the associated components, interfaces, and reference points. The reference model is independent of any specific technology. Standardized mechanisms will facilitate large-scale machine-to-machine communication and help with the integration between OCN and the Internet.

Discussion Venues

This note is to be removed before publishing as an RFC.

Discussion of this document takes place on the Internet Area Working Group Working Group mailing list (int-area@ietf.org), which is archived at https://mailarchive.ietf.org/arch/browse/int-area/.

Source for this draft and an issue tracker can be found at https://github.com/kiranmak/draft-kmak-ocn.

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction
2. Terminology
  2.1. Acronyms
3. Operation and Control Networks
  3.1. Definition
  3.2. Reference Model
    3.2.1. Controller Point (CP)
    3.2.2. Actuation Point (AP)
    3.2.3. Sensor Point (SP)
4. OCN Communication Interfaces
  4.1. Actuator Point Interface
  4.2. Sensor Point Interface
  4.3. Application Interface
5. OCN Characteristics
  5.1. OCN Message Classification
    5.1.1. In-time messages
    5.1.2. Bounded latency messages
    5.1.3. On-time messages
    5.1.4. Periodic messages
    5.1.5. Order of messages
  5.2. Other Characteristics
    5.2.1. Reliability
    5.2.2. Safety
    5.2.3. Synchronization
    5.2.4. Security
    5.2.5. Privacy
6. OCN Examples and Realizations
  6.1. Physical Layer
  6.2. Link Layer
  6.3. Network Layer
7. IANA Considerations
8. Security Considerations
9. Acknowledgements
10. Informative References
Authors' Addresses

1. Introduction

A number of applications require specialized networks to perform operations that change or monitor the behavior of equipment and the environment in which they operate. Such application domains benefit from software-driven process automation with the ability to control and detect changes remotely.

Traditionally, equipment related control processes and monitoring mechanisms are associated with the production plants and manufacturing environments. Moreover, growth in the Internet of Things (IoT) has broadened the role of operations, control, and process automation into a diverse set of market verticals and commercial applications.

For example, residents can control door locks remotely at home and can observe visitors at the door with the surveillance cameras. Networks with in a vehicle are used to coordinate the entire engine operations including speed control, tire pressure, collision detection, and avoidance mechanisms. These operations are performed through intelligent software without human-in-the-loop. In a large-scale energy power distribution system, control units in substations monitor real-time power consumption and perform automatic load re-distribution across different sub-stations to prevent outages.

The scenarios described above are common in the sense they all involve operating an equipment (such as a machine) through communication between a controller device (e.g. PLC) and an actuating or a sensing device.

The essential characteristics of networks between these devices are delivery of a command to a machine with high-precision, its safety, reliability and security. This implies low or no tolerance to latency and packet losses (among other things covered later).

Since there are several such applications, a common connectivity interface is required between the different components.

An Operation and Control Network (OCN) is the interconnection of field devices (actuators, sensors) and their associated controllers to exchange data to cause and monitor changes to the end-equipment. Each OCN connection is designed or provisioned to fulfill the traffic characteristics with stringent time and reliability constraints such as protecting bounded latency and not allowing packet losses.

OCN, itself is not a new concept in itself. Other industrial network technologies that would be classified as OCN are available, albeit with limited functionalities and at a smaller scale. Whereas, demand for improvements in process automation at a large scale is growing across diverse applications. Thus, a broader and more generalized approach will benefit several industry verticals.

OCN integrates automation infrastructure beyond a single location to multiple sites and even to the cloud; it additionally integrates existing industrial network technologies. OCN aims to formalize the mechanisms for interaction between the OCN components.

The rest of the document represents the OCN taxonomy and a detail description of OCN concepts.

2. Terminology

*Operational technology (OT): Programmable systems or devices that interact with the physical environment (or manage devices that interact with the physical environment). These systems/devices detect or cause a direct change through the monitoring and/or control of devices, processes, and events. Examples include industrial control systems, building management systems, fire control systems, and physical access control mechanisms. Source: [NIST-OT]

*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 which 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.

*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 fieldbus devices, digital controllers and software applications

*Human Machine Interface: An interface between the operator and the machine. The communication interface relays I/O data back and forth between an operator's terminal and HMI software to control and monitor equipment.

2.1. Acronyms

- HMI: Human Machine Interface
- OCN: Operations and Control Networks
- PLC: Programmable Logic Control
- OT: Operational Technology

3. Operation and Control Networks

3.1. Definition

The Operations and Control Networks are defined as follows:

> An Operation and Control Network (OCN) is 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.

An OCN is 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.

> Note: the term "OCN field device" will be used to represent actuator and sensors together.

OCN relates to Operational Technology (OT) in ICS and extends it. While OT networks are commonly engineered over a limited physical range in a geographic area, OCNs improve upon conventional OT by supporting large-scale network layer connectivity paradigms. Logically, OCNs facilitate connectivity across larger geographical areas, for instance, beyond factory premises covering several cloud and edge scenarios in which components are disaggregated or are not co-located. Of course, physical distance limits still apply to applications with strict requirement of control command completion.

OCN provides inter-networking or mechanisms to interact between controlling and monitoring components (that maybe remote) with the field devices close to the operating machinery and the equipment.

The OCNs support different types of messages across these function elements. The message data sent from controller to actuator is smaller than a typical network payload. Packet delivery must be guaranteed by the OCN. Additionally, the OCN should support and advertise mechanisms to eliminate packet losses.

Most common attributes among OCN enabled applications are different types of guarantees of time for different operations, safety of those operations, and the reliability of data delivered. In addition security and privacy are also more critical than the general-pupose applications. These characteristics are covered in Section Section 5.

3.2. Reference Model

The following three reference points for OCNs are of interest: Actuator Point, Sensor Point, and Controller Point.

Note: Suggestions on naming anything is OK. I am not happy with any of these names.

```
         +----------+ +---------+
         | Actuator | | Sensor  |
         | Point    | | Point   |
         +---^------+ +------^---+
             |               |
             |AP-I           | SP-I
         +---v---------------v-----+
         | Operations & Control    |
         |       Network (OCN)     |
         +-----------^-------------+
                     |
             +-------v------+
             | Controller   |
             |   Point      |
             +--------------+
                   ^
                   | API
                   V
             ---------------
             | Applications |
             ---------------
```

Figure 1: Operations & Control Networks(OCN) - Reference Model

An 'operation' in OCN can be any of the following -

*accessing information from the field-sensors,

*writing command data,

*reading back from the actuators.

The Figure 1 above is a reference model for the OCN. An application executes operation on field-devices over OCN to monitor specific and/or overall state of the system; An operation may involve realizing feedback control loop between the controller, actuating and sensory devices.

The OCN Reference model is extended to accommodate a variety of access networks. In fact, it serves as convergent network to integrate communication across different technology specific networks. Consider it as a specialized network infrastructure (shared or dedicated) that interconnects different other OT-enabled access networks. Some of the examples of OT-enabled networks are Ethernet/IP, Profinet, TSN [TSNTG], Detnet[DETNET-ARCH], 5G radio, private 5G, etc. As is implied that each of these technologies are by themselves capable of supporting some of the properties of OCN which in turn provides a comprehensive approach to integration of these technologies at large-scale to build a converged framework.

A generalized OCN model supports the following logical connection points:

3.2.1. Controller Point (CP)

A controller point is a logical entity authorized to interface with the sensors and actuators over the OCN. The CP has the knowledge of an application's performance parameters which are expressed in terms of network specific requests or resources such as, tolerance to packet loss, latency-limits, jitter variance, bandwidth, and specification for safety. The CPs should have knowledge about these capabilities from the OCNs in order to meet their packet delivery constraints. Since OCNs are expected to be shared among different applications with their own set of KPI, a controller should be used to express its specific requirements in the OCN. Moreover, each command from controller may have to indicate its own KPI.

An important aspect of the controller function element is that it integrates with the application infrastructure and provides a standard interface with them. Optionally, it may be an application in itself.

3.2.2. Actuation Point (AP)

An actuation point is the functional element which receives actuator specific commands and is used for the communication between the actuator devices and controllers. The OCN enables control of actuating devices remotely from the controller by meeting all the requirements (KPIs) necessary for a successful command execution.

The actuator participates in closed control loop over OCN with CP when necessary.

The standard network specific interface between the controller and actuator is called AP-I (see Section 4.1).

3.2.3. Sensor Point (SP)

The sensor point is the point where sensor connects to. Its main function is to emit periodic data from the sensors. It may intermittently provide asynchronous readings upon request from the controller.

A sensor point is the functional element from where sensory data is emitted back to controller. SP may receive initial requests to emit data with certain periodicity or may provide realtime data upon request. The communication to sensor is also through a controller since controller is involved in using sensory data to change parameters in actuators.

The OCN enables delivery of data emitted from sensor devices to the controller networks by meeting all the application demands in particular periodicity and severity of the observed data. The standard network specific interface between the controller and sensor is called SP-I (see Section 4.2).

4. OCN Communication Interfaces

OCN interfaces enable communication between its reference points; two specific interfaces are defined below. Additionally, an application to CP interface is also anticipated to express application logic.

4.1. Actuator Point Interface

Interface between CP and AP is called AP-I. It carries out communication between the actuation points and the controller points. The Actuators are designed to receive "control command" from controllers and perform corresponding action or change to the equipment. Those commands can be abstracted as writes and then read-back of values. Thus, the message may be request write and then request read-back in reply. The high-precision timing and delivery of such messages must be met in either direction independently. This interface is a bidirectional and the model allows more than one controller interacting with the AP.

4.2. Sensor Point Interface

Interface between CP and SP is called SP-I. It describes the set of messages permitted between the sensor points and controller points.

The Sensors may be programmed to send periodic sensory data at specified intervals. There may also be other cases, in which the controller may .solicit reading values. The interface should be a bi-directional and more than on controller can request sensor data.

```
                  .-,,-.
   +--+        .-(  O   )-.       +--+
   |  |<-------;--+ C +----;----->|  |
   +--+  AP-I  '-(| N | ).-'SP-I  +--+
    AP            |...|            SP
                  |   |
                +-v---v+
                |  CP  |
                +------+
                   | Application interface
             +-----v--------+
             | Applications |
             +--------------+
```

Figure 2: Interfaces in OCN

Note: Direct sensor to actuator communication is not in the scope of OCN for the following reasons:

1. In this model, actuator and sensors do not have 'decision-making' capabilities. They perform requested tasks as instructed. In other words, they are passive actors. The tasks performed by these field-devices themselves maybe autonomous but do not change their behavior or react to changing conditions once programmed. Providing a direct communication between sensor and actuator could potentially leave controller out-of-sync or the operations in unpredictable state.

2. It is likely that several applications are interested in reading sensors for offline analysis and do not intend to changes the state in control processes. For such cases, it helps to have limited set of permitted messages and prevent from executing undesirable actions.

4.3. Application Interface

An application domain combines everythin - the application logic, group of actuators, sensors and one or more controllers. With in the application domain the interface between controller and application logic is called application interface (API). The API allows applications to request specific outcomes or data from the field devices through the CPs. It is possible to have controller point embedded in an application, in such cases this interface may not be needed.

5. OCN Characteristics

The characteristics of OCN differentiate it from the general purpose networks of today which provide the end user (humans or non-critical applications) connectivity to a plethora of services (web, media streaming, data transfers, e-commerce etc), rarely involving machine-to-machine type communications.

These characteristics include the type of communication messages and other key aspects of OCNs.

5.1. OCN Message Classification

The OCNs are designed for the real-time applications with the assurance of successful command delivery. The time or high-precision requirements can be classified in three different ways - in-time (the message arrives before a specified time), on-time (the message arrives exactly at the specified time) and bounded time (the message is arrives in a given range of specified time window).

Another consideration about the message delivery in OCNs concern with the target of a message, i.e. that parameter represents communication time or processing time i.e. an end-to-end execution of commands.

The functional behavior of OCN can be explained through classification of messages as described below.

5.1.1. In-time messages

In-time messages supply data to receivers before the specified time parameters. The messages may originate from either direction. i.e., controller to field devices or vice-versa. Controller to/from field device messages must reach with in the specified time. An in-time request originating from the controller to actuator will specify the maximal delay permissible time, in which requested operation must take place.

> Note: todo - The OCN must support mechanisms related to relative time knowledge across the domain. However those mechanisms are out of scope of this document.

5.1.2. Bounded latency messages

Bounded latency message requests correspond to a given the earliest and the latest arrival time, or a range of time in which that operation must take place. This type of request is different from in-time messages because of the additional constraint that message should not be processed too early but processed in a given interval.

5.1.3. On-time messages

The on-time messages supply data at a specific time with tolerance for only a very small difference (in terms of measurable unit) between the earliest and latest time-values. On-time message guarantees complement in-time services. On-time messages, for example, must ensure that the actuator executes the command at the time requested and not before or after.

It is different from the bounded latency and in-time messages. In-time messages, may arrive and are valid anytime before the requested parameter. The on-time constraint is that message must not be processed before the requested value. Ideally, on-time request will have same earliest and latest values. If OCN delivers or the AP processes message before the specified time then it is an error and may leave system in an undesirable state.

5.1.4. Periodic messages

Sensors emit data at regular interval but this type of information may not be always time-constrained but gaps between the period can provide an indication to the controller about the communication or other problems.

5.1.5. Order of messages

In OCN where real-time communication is the key characteristic, out of order message processing will lead to failures and shutdown of operations. Messages may be correlated therefore, time constraints may be applied on a single message or a group of messages.

5.2. Other Characteristics

The use cases related to OCN have more stringent and finer grained demands from the networks and some of the characteristics are difficult to express as quantifiable parameters.

5.2.1. Reliability

Reliability is characterized by OCN's ability to deliver a packet successfully with the specified criteria. OCN may implement different strategies to improve network reliability in response to router or link failures. Some of those strategies include - providing redundant paths, avoiding congestion, use of reliable media or implementing mechanisms in software.

It is a combination of

- *topological reliability - i.e. having one of more paths with same packet delivery constraints.

- *stability reliability - i.e. minimizing variations in packet delivery patterns (in terms of time, path) between two adjacent packets with the same constraints.

- *forwarding reliability - i.e. replicating packets in the network to minimize packet losses.

An OCN should provide sufficient telemetry data about the changes or anomalies in OCN as well as reasons at its earliest when it was unable to deliver packets in a requested fashion.

> Note: OCN may be required to report a packet loss back to application immediately instead of relying on conventional end-to-end transport mechanisms.

5.2.2. Safety

Safety implies several things - that the requested operation or a control command was executed as instructed without any adverse impact to the mechanical equipment or the environment.

The traffic originating from change is triggered through commands delivered to actuator and the same device or different sensor Each OCN connection is designed or provisioned to fulfill the traffic-characteristics with stringent quality of services.

5.2.3. Synchronization

In order to support high-precision of time, some applications may use network clock synchronization protocols such as PTP [PTP-GRID]; while some other applications rely on GPS clocks. Remaining applications may not use the clock synchronization at all and rely on other logical methods. OCN should provide accurate delivery of packets through which ever methods and those methods should be opaque to the applications.

5.2.4. Security

5.2.5. Privacy

6. OCN Examples and Realizations

This section discusses different types of OCNs. This section is include to appreciate the need for OCNs. OCN networks may be deployed at different network layers as discussed below.

6.1. Physical Layer

An OCN network may be implemented fully on the layer one of the protocol stack. It is the most trivial example of an operations and control in which an actuator or sensor is directly accessed from a controller. For example, turning the switch on or off manually, turns a bulb, fan, etc on/off. The field-devices are connected to controller directly over a wire. Such type of scenarios are not part of the OCN, as there is no network involved.

6.2. Link Layer

An OCN network may be implemented on the layer 2 as a local area network. In factory floors or plants, recently realtime Ethernet networks are deployed to meet some of the characteristics of OCN. The layer 2 solutions are difficult to extend and generalize beyond a certain distance. It is difficult to easily integrate cloud-based remote control and operations specific use cases in such cases.

Other media options include 5G radio communications that also support many of the OCN attributes. Furthermore, OCN could complement these access network technologies by connecting them over wide areas for edge and cloud related accesses.

6.3. Network Layer

Support for large scale OC solutions requires support for all the characteristics end-to-end which may include crossing through different networks as well as interconnection of operations and control access networks over the internetworks while meeting all the requirements. OCNs aim to achieve this. i.e., providing a network level approach to connecting sensors, actuators and controller from anywhere and meeting application constraints.

An OCN may be implemented in the layer 3 using packet switching technologies and protocols. The layer-3 OCN requires support for all the characteristics of messages as described above, especially for real-time end-to-end timing constraints. Layer-3 OCNs may be deployed as a single autonomous system or as part of a single autonomous system. It may involve crossing through different networks as well as interconnection of operations and control access networks while meeting all the requirements. Layer 3 OCNs are aimed at large-scale, in comparison with Layer 2 OCN, and physically distributed manufacturing facilities and/or applications involving end devices of frequent mobility.

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

[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/rfc/rfc8655>.

[NIST-OT] Initiative, J. T. F. T. and National Institute of Standards and Technology, "Risk management framework for information systems and organizations:", DOI 10.6028/nist.sp.800-37r2, <http://dx.doi.org/10.6028/nist.sp.800-37r2>.

[PTP-GRID] IEEE, "IEC/IEEE International Standard - Communication networks and systems for power utility automation – Part 9-3: Precision time protocol profile for power utility automation", DOI 10.1109/ieeestd.2016.7479438, <http://dx.doi.org/10.1109/ieeestd.2016.7479438>.

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

Authors' Addresses

Kiran Makhijani
Futurewei

Email: kiran.ietf@gmail.com

Tooba Faisal
King’s College London

Email: tooba.faisal@kcl.ac.uk

Richard Li
Futurewei

Email: richard.li@futurewei.com