Workgroup: Detnet Group
Internet-Draft: draft-km-detnet-for-ocn-00
Published: 13 March 2023
Intended Status: Informational
Expires: 14 September 2023
Authors: K. Makhijani T. Faisal R. Li
Futurewei King's College London Futurewei
C. Westphal
Futurewei

Using Deterministic Networks for Industry Operations and Control

Abstract

Remote industrial process control & operations improve automation, resource efficiency, safety and better overall control from the software-defined application logic. So far, industrial/process automation connectivity is mostly localized. In order to use cloud-based connectivity, not only deterministic networks are needed but an interface between the endpoints and the DetNet is required to be clearly described. This document describes an interface to deterministic networks from the view of end-points to support process control and operations.

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

Traditional industrial networks are designed to support process automation within a production plant or a manufacturing floor. Therefore, the network was typically a campus-area, local network and it played an important but not a critical role. Now, as equipment control and monitoring become remotely supported from the cloud or the edge, network technologies such as TSN, and DetNet in particular, are gaining relevance.

Process automation systems involve operating a piece of equipment (such as actuating and/or sensing field-devices. The communication between the controllers and field-devices exhibits a well-defined set of behaviors and has specific characteristics: the delivery of a control-command to a machine must be executed within the time-frame specified by a controller or by an application to provide reliable and secure operation. A low or zero tolerance to latency and packet losses (among other things) is implied. In this document, these special purpose networks are referred to as operation and control networks (OCNs) [OCN-MODEL].

DetNets provide mechanisms for guaranteed packet delivery in-time, for reliability, and for packet loss mitigation. Thus, the OCNs are an application's view of a network and DetNet is one of the potential underlying enabling technology.

The packet processing in DetNet is associated with a flow. A DetNet service deals with aggregated flows for which a network service provider would engineer and allocate resources. Thus, the networks are provisioned for less dynamic (long-lived) scenarios. However, OCN-type traffic patterns arise from the programmatic behavior of an application. Hence they can be dynamic, sporadic and intermittent. This leads to the issue of how applications can interact with the DetNet-enabled networks.

This document outlines the opportunities to make DetNet more amenable to OCN environments, by describing the interface between the OCN application and DetNets i.e., using DetNet services for communication between the controllers and the field-devices. This interface is used by an application to express its network-specific requirements. The document presents the perspective of an end-system that is a 'process-control & operation' type of cloud-hosted application. Because most cloud-hosted applications would rely on IP, we consider first these specific to IP-enabled DetNet data planes [DETNET-DP]. Hence the discussions will assume IP-base end-systems. For the other type of end-systems, the field-devices, service level proxy functions are assumed (as per section 4.1 in RFC8655).

The rest of the document presents a special case of DetNet referred to as Operation and Control Networks (OCN). Section 3 provides a background on the type of traffic for OCN applications. In the context of interface between an application and DetNet, some of the limitations in IP-enabled Detnets are covered in Section 4. The document is intended to discuss possible approaches or potential solution direction to support OCN traffic patterns over DetNet, as covered in Section 5.

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 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 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: A feedback loop is part of a system in which some portion (or all) of the system's output is used as input for future operations.

*Industrial Control Networks: Industrial control networks are the interconnection of equipment used for the operation, control or monitoring of machines in the industry environment. It involves a different level of communication - between fieldbus devices, digital controllers and software applications

*Human Machine Interface (HMI): 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

*OC: Operation and Control

*OCN: Operation and Control Networks

3. Background on Industrial Control Systems

An industry control network interconnects devices used to operate, control and monitor physical equipment in industrial environments. Figure 1 below shows such systems' reference model and functional components. Closest to the physical equipment are field devices (actuators and sensors) that connect to the Programmable Logic Controllers (PLCs) or other types of controllers using serial bus technologies (and now Ethernet). Above those controllers are Human Machine Interface (HMI) connecting different PLCs and performing several controller functions along with exchanging data with the applications.

A factory floor is divided into cell-sites. The PLCs or other types of controllers are physically located close to the equipment in the cell-sites. The collection of monitoring, status and sensing data is first done on the site and then transmitted over secure channels to the cloud applications.

```
     +-+-+-+-+-+-+
  ^  | Data Apps |....            External business-logic
  :  +-+-+-+-+-+-+   :                Network
  :        |         :
  v  +-+-+-+-+-+-+  +-+-+-+-+--+
     | vendor A  |  |vendor B  |  Interconnection of
     | controller|  |controller|  controllers
  ^  +-+-+-+-+-+-+  +-+-+-+-+-+   (system integrators)
  :       |         |
  :   +-+-+-+-+  +-+-++-+
  :   | Net X |  | Net Y|
  v   | PLCs  |  | PLCs |--+    device-controllers
  ^   +-+-+-+-+  +-+-+--+  |
  :      |        |        |
  :   +-+-+    +-+-+    +-+-+
  v   |   |    |   |    |   |   Field devices
      +-+-+    +-+-+    +-+-+
```

Figure 1: Functions in Industrial Control Networks

What is changing now is that cloud applications are integrating process control functions to improve automation and to make real-time decisions, programmatically. The equipment control and collection of data generated by the sensors can be done directly over DetNet-enabled wide-area networks as illustrated in Figure 2.

```
               +-+-+-+-+-+-+-+-+
               |     Data Apps |      Integrated Apps with
               | c1 | c2  | c3 |      Remote process control
               +-+-+-+-+-+-+-+-+
                \   ,-----.   /
                 +-[  Det- ]-+
                   [Network]
                    `-----'
               +-+-+-|  |-+-+-+-+
               |        |       |
             +-+-+    +-+-+   +-+-+
             |   |    |   |   |   |   Field devices
             +-+-+    +-+-+   +-+-+
```

Figure 2: Converged Cloud based Industrial Control Networks

One particular motivation is to provide the behavior of a serial bus between the cloud and the actuators/sensors with the same assurance of reliability and latency, albeit over wide-area networks (WAN). This is evident from many Industry control applications, such as factory automation [FACTORY], PLC virtualization [VIRT-PLC], power grid operations [PTP-GRID], etc. that are now expected to operate in the cloud by leveraging virtualization and shared infrastructure wherever possible.

3.1. Connected Controllers, Sensors and Actuators

Control systems comprise Controllers, Sensors and Actuators. The data traffic essentially carries instructions that cause machines or equipment to move and do things within or at a specific time. The connectivity exists in the following manner:

*A controller interfaces with the sensors and actuators. The controller knows 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 controller knows all the packet delivery constraints.

*An actuator receives specific commands from the controllers. The DetNet should be able to enable control of actuating devices remotely from the controller while meeting all the requirements (or key performance indicators - KPIs) necessary for successful command execution. The actuator participates in a closed control loop as needed.

*A sensor emit periodic data from the sensors. It may intermittently provide asynchronous readings upon request from the controller. Sensors may report urgent messages regarding malfunctioning in certain equipment, cell-sites, or zones.

Almost all control systems have at least one controlling entity on one end, and two other end points - the sensors and actuators. The interface to sensors and actuators is through the controllers; i.e., applications do not directly interact with the field-devices. Neither actuators nor sensors perform decision-making tasks. This responsibility belongs to the controller.

3.2. Traffic Patterns

For either local or wide area, the process automation activities over the network can generate a variety of traffic patterns between the controllers and field-devices such as:

3.2.1. Control Loops

The equipment being operated upon is sensitive to when a command request actually executes. An actuator upon receiving a command (function code) will immediately perform the corresponding action. It is the responsibility of network and controller to ensure that behavior of the sensor and actuator follows the expectations of applications.

For several such applications, the knowledge of a successful operation is equally critical to advance to the next steps; therefore, getting the response back in a specified time is required, leading to a knowledge of timing. These types of bounded-time request and response mechanisms are called control loops.

Unlike general purpose applications, commands cannot be batched, the parameters of the command that will follow depends on the result of the previous one. Each request in control loop takes up a minimal payload size (function code, value, device or bus address) and will often fit in a single short packet.

In Detnet-enabled network, it can be imagined as a small series of packets with the same flow identifier, but with different latency constraints.

It is required to support control loops where each request presents its own latency constraints to the network and where commands are small sized packets.

3.2.2. Periodicity

Sensors emit data at regular intervals, but this information may not always be time-constrained. Usually, controllers are programmed to tolerate and record intermittent losses. Automation software can make a more informed decision by monitoring a lot of sensor data. Thus, the traffic volume generated by sensors is expected to high. The periodicity of each sensor can also vary based on the equipment.

It is required that network capacity is planned appropriately for the periodic traffic generated from the different sensors. The periodic interval should also be preserved in the network because any variations could provide false indications that the equipment is misbehaving.

3.2.3. Ordering

In real-time process control communications, out of order message processing will lead to costly failures of operations. Messages such as request and reply, or a sequence of commands may be correlated therefore, both time constraints and order must be preserved. The traffic is generated when software triggers control-commands to field-devices. This may not always map into asynchronous DetNet flows if observation interval is not known.

The network should be capable of supporting sporadic on-demand short-term flows. This does not imply instantaneous resource provisioning, instead it would be more efficient if the provisioned resources could be shared for such asynchronous traffic patterns.

Another consideration with ordering is that both actuators and sensors are low-resource devices. They can not buffer multiple packets and execute them in order while maintaining the latency bounds of each command execution. This means the network must pace packets that may arrive early.

3.2.4. Urgency

Besides latency constrained and periodic messages, sensors also report failures as fault notifications, such as pressure valve failure, abnormally high humidity, etc. These messages must be delivered with utmost urgency and immediately.

3.3. Communication Patterns

Control systems follow a specific communication discipline. The field-devices (sensors and actuators) are always controlled, i.e., interact with the system through controllers in the following manner:-

- Sensor to controller: data emitted at periodic interval providing status/health of the environment or equipment. The traffic volume for this communication is determined by the payload size of each sensor data and the interval. These are a kind of synchronous

Detnet flows but with much higher time intervals; still the inter-packet gap should be minimum.

*Controller to/from actuator: the commands/instructions to write or read. Actuators generally do not initiate a command unless requested by the controller. Actuators will often execute a command, read the corresponding result, and send that in response to the original write command. The traffic profile will be balanced in both directions due to requests/ response behavior. These are like asynchronous flows but without the observation interval constraint.

4. Gap Analysis

Today, most of the operations and control solutions are split approaches. This means that the controller is on-premises close to the equipment, sensor data is also collected on-site and then transmitted to the cloud for further processing.

To support delivering remote instructions to the machines over wide-area networks using Deterministic Network data plane architecture [DETNET-DP] and corresponding data plane DetNet over IP [DETNET-IP] mechanisms apply as discussed in Section 4.1. Later in Section 4.2 additional asks from DetNet are covered.

4.1. Deterministic Networks Relevance

Note: This section's text and explanation on DetNet can be removed.

```
 DetNet IP       Relay                        Relay       DetNet IP
 End System      Node                         Node        End System

+----------+                                             +----------+
|   Appl.  |<------------ End-to-End Service ----------->|   Appl.  |
+----------+  ............                 ...........   +----------+
| Service  |<-: Service  :-- DetNet flow --: Service  :->| Service  |
+----------+  +----------+                 +----------+  +----------+
|Forwarding|  |Forwarding|                 |Forwarding|  |Forwarding|
+--------.-+  +-.------.-+                 +-.---.----+  +-------.--+
         : Link :       \      ,-----.      /     \   ,-----.   /
         +......+        +----[  Sub- ]----+       +-[  Sub- ]-+
                              [Network]              [Network]
                               `-----'                `-----'

         |<--------------------- DetNet IP --------------------->|
```

Figure 3: A Simple DetNet-Enabled IP Network, Ref. RFC8939

Figure 3 is described in the DetNet IP dataplane [RFC8939] and illustrates a DetNet-IP network. The DetNet-enabled end systems originate traffic encapsulated with Detnet forwarding and service sub-layers; otherwise some attached relay node will create the Detnet sub-layers based on information received from the end system. The forwarding sub-layer is responsible for resource allocation and explicit path functions, whereas the service sublayer provides packet replications, sequence numbering, and other functions. Within the Detnet nodes, resources are allocated a priori for a flow.

The DetNet supports both asynchronous (by allocating resources for the observation interval) and synchronous (with repeating schedules) flow behaviors (Section 4.3.2 in [DETNET-DP]). The granularity of DetNet services is at the flow level (6-tuple flow, including DSCP).

Realistically, leveraging DetNets for Operations and Control (OCN) traffic patterns Section 3.2 can be challenging for the reasons described next.

4.2. DetNet related Considerations and Dependencies

Per the Detnet architecture, a DetNet-aware node should express the network requirements as part of forwarding sublayer or service-sublayer. The [DETNET-IP] spec doesnot specify how sublayers are mapped in 6-tuple flow.

In case of operations & control-application, a DetNet service consumer will need to provide a service-level manifest to the DetNet service provider (DN-SP) for each controller and field-device pair. The DN-SP is expected to allocate resources and return a mapping of a DSCP (DetNEt Qos) for each pair. This could be become a scaling problem as the number of controller-device pairs start to grow.

Given that only DSCP is available, field-device pair can pose issues such as:

*How can application request the proper network-resource for each command?

*How can an application receive periodic data from sensors?

*What are the ways to differentiate a less sensitive (periodic) updates from urgent alarms.

*Or how to differentiate data received from a sensor or actuator and process them accordingly.

These issues are described below in more detail.

4.2.1. Operator vs Application view

The DetNet data plane is designed with a network-operator-centric approach. In order to use resources efficiently, there is an emphasis on aggregation of several flows together. The operators in Industrial control networks are not necessarily network experts; they will face complexities in presenting a request to the DetNet forwarding engine. Especially, an application is written to control a set of field-devices and monitor a different set of sensors and will need to learn the mappings for each controller-field-device (ctrl-flddev) pair to the applicable DetNet flows.

As the number of ctrl-flddev pairs grow, their variable traffic profiles can become hard to manage.

An OCN application is unaware of how DetNet services are provisioned. A common UNI between the applications and DetNet-enabled network needs to be added to the current framework to better map the expectations better.

4.2.2. Flow reservation and classification

Inside the DetNet, flow identification is done using IP header and DSCP information. These flow identifiers are then used by DetNet nodes to provide the corresponding traffic treatment. Accordingly, resources are provisioned over longer timescales, i.e., the model works for relatively predictable scenarios. The problem is that the control loops in Section 3.2.1 may be short messages so that one command is sent per packet, expecting a response from the actuator in another return packet. The transmission of the next set of commands is driven programmably by the applications. This is how the softwarization of industrial processes is happening now.

Perhaps, it can be stated that the provisioning resources for flows does not necessarily guarantee that the Detnet-specific resource contention at the instant will not occur.

Moreover, for any cloud-based solution, controller may as well send commands to the devices from different locations (different IP addresses), thus the scale of provisioned flows can grow very fast.

To utilize Detnet-specific resources, it is needed to embed specific information in addition to DSCP, so that dynamic traffic patterns can be scheduled deterministically.

4.2.3. Split Traffic flows

One of the most constrained design elements in today's industrial control systems is that data from the sensors is collected on-site and often aggregated before transporting to the cloud. Historical reasons for this approach do not apply anymore. Due to growth in sensor data, it now requires a much larger on-site storage infrastructure which is expensive. Applications also expect real-time streaming telemetry data. Although latency constraints are not as strict as for control loops, sensor data need to preserve periodicity (Section 3.2.2), and also requires DetNet service support.

Leveraging DetNet could eliminate split traffic flows by collecting the sensor data by the applications. This also allows controllers to be run and operated from the cloud platforms where much more powerful compute capabilities and available.

4.2.4. Provisioning for variety of Traffic flows

Different operational scenarios have different constraints; even commands within the same application will have different time requirements.

- Different types of latency bounds will be required between a controller and an actuator pair based on the type of end-equipment and precision requirements. Out-of-order message processing may lead to failures and shutdown of operations. Messages may also be correlated. Therefore, time constraints may be applied on a single message or on a group of messages.

- Similarly, each sensor-controller pair may come with its own interval requirement. Sensors emit data at regular interval but this type of information may not always be time-constrained. The gaps between the period can provide an indication to the controller about communication or other problems.

- Additionally, some faults and alarm messages are urgent reports and must be marked and transmitted accordingly.

It is not clear if all these variations can be predictably resolved without any additional information offered to the DetNet forwarding plane. For example, if two independent OCN flowlets (that is, ordered group of packets that are related at process control logic) with variable bounded latency are classified to the same DetNet flow, they will receive the same treatment, regardless if one has the shorter latency than the other and may end up behind a flowlet with longer latency value. On the other hand, if an OCN flowlet have packets with different latency values, they could end up in different DetNet flow and may not reach destination in a specific order.

4.2.5. Security

Industry control networks also have split security boundaries. They have been designed to be air-gapped or secure by separation. Current systems have strict admission control, ingress and egress policies.

From network layer security perspective, how DetNet-enabled network deals with security falls in the [RFC9055], the end-systems expect those mechanisms in place. In particular if additional information is distributed for datapath decisions, integrity protection as per Section 7.2 of [RFC9055].

The border gateways and firewalls will be more prone to errors related to provisioning churns if the system is dynamic or continuously changing.

The transport layer deals with the end-to-end encryption. It should evolve to incorporate additional IoT-friendly(lightweight) protocols such as COAP, MQTT and their encryption mechanisms.

4.3. Summary of Gaps

*Application view (Section 4.2.1: An OCN application is unaware of how DetNet services are provisioned. A common UNI between the applications and DetNet-enabled network needs to be added to the current framework to better map the expectations better.

*Security (Section 4.2.5): of process control related metadata to be used by network must be secured.

*Traffic behavior (Section 4.2.4 and Section 4.2.2): Within the same DetNet flow, classified via 6-tuple, additional information/ metadata must be supported so that dynamic traffic patterns can be scheduled deterministically.

*Split traffic (Section 4.2.3): Leveraging DetNet should eliminate split traffic flows by direct collection of sensor data by the applications. This also allows controllers to be run and operated from the cloud platforms where much more powerful compute capabilities are available.

5. DetNet Potential Approach

Remote process automation presents different types of traffic profiles and to deal with them within the DetNet framework, we discuss few possibilities.

The DetNet UNI will enable applications to convey specific requirements to DetNet-aware Network. Note, that it is just an interface and blind to the internal implementation of such networks.

The DetNet architecture does not describe how DetNet-aware node can design DetNet sub-layers. But even from the view of an end-system the separation between forwarding and service sublayer functions should be maintained. This means, the DSCP should not be overloaded and DetNet-IP forwarding layer should be extended.

5.1. Application association to Forwarding sub-layer

Applications should convey specific resource requirements to the DetNets they connect to. There are two potential options: (a) The DetNet Relay-node performs translation and binding to one of the DetNet services in the DetNet; or (b) or carry the application defined data over DetNet as is and enable processing on transit nodes.

5.2. Encapsulation

Note that the applications in this context are in the cloud, IP is expected for the end-stations (MPLS DetNet will not apply). It is also reasonable to assume that the data plane is IPv6 and extension headers are used for support in DetNet.

The end-system network requirement is expressed as 'Flowlet or Packet Level QoS'. Each packet carries its own unique QoS. The meta data to be transmitted to DetNet are:

- Async traffic with latency-information.
- Sync, periodic traffic
- urgency of messages
- Flowlet identification (for related packets).

This can be implemented using the HBH extension header option.

5.3. Operation and Control Network Option (OCNO)

The OCN Option (OCNO) is a hop-by-hop option that can be included in IPv6 for OCN traffic control extensions.

```
    0                   1                   2                   3
    0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
                                   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
                                   |  Option Type  |  Opt Data Len |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   | OCNF flags     |   OCN-TC-Flowlet nonce       |  sequence     |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |                (bounded latency spec)                         |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |                (Delay variation spec)                         |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 4: Explicit Traffic Control HBH Options

Option Type:

8-bit identifier of the type of option. The option identifier for the OCN Option (0x??) to be allocated by the IANA. First two bits will be 00 (skip over this option and continue processing the header.)

Option Length:

8-bit unsigned integer. Multiple of 8-octets.

OCN Function Flags:

Some flags require metadata, others dont. So process flags in order, if the flag is off, following metadata will not be present.

Flag	Description
U	send message immediately. its an alarm
P	periodic packet (intervals in ~ms)
F	part of flowlet. see Nonce and seq
L	bounded latency spec provided
R	Reliability with no packet loss tolerance
V	Delay variation with no packet loss tolerance

Table 1

Flowlet nonce:

16-bit. identifies that a packet is associated to group of packets and shares fate.

Flowlet sequence:

8-bit. sequence to be used for ordering with in flowlets.

Bound Latency Spec:

32-bit. Encodings, to be defined.
16-bit (upper bound), 16-bit (lower-bound). This field will provide upper and lower latency bounds describing the the latency bounds in milliseconds corresponding to the packet.

Delay Variation Spec:

16-bit. for synchronous stream, delay variation tolerance in ms.

6. IANA Considerations

TBD

7. Security Considerations

See section on security above.

8. Acknowledgements

9. References

9.1. Normative References

[DETNET-DP] 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>.

[DETNET-IP] 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/rfc/rfc8939>.

[RFC8939] 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/rfc/rfc8939>.

[RFC9055] Grossman, E., Ed., Mizrahi, T., and A. Hacker, "Deterministic Networking (DetNet) Security Considerations", RFC 9055, DOI 10.17487/RFC9055, June 2021, <https://www.rfc-editor.org/rfc/rfc9055>.

9.2. Informative References

[FACTORY] Westphal, C., Makhijani, K., Dev, K., and L. Foschini, "OCN Use Cases for Industry control Networks", Work in Progress, Internet-Draft, draft-wmdf-ocn-use-cases-00, 7 July 2022, <https://datatracker.ietf.org/doc/html/draft-wmdf-ocn-use-cases-00>.

[NIST-OT] "Risk management framework for information systems and organizations:: a system life cycle approach for security and privacy", National Institute of Standards and Technology report, DOI 10.6028/nist.sp.800-37r2, December 2018, <https://doi.org/10.6028/nist.sp.800-37r2>.

[OCN-MODEL] Makhijani, K., Faisal, T., and R. Li, "Operations and Control Networks - Reference Model and Taxonomy", Work in Progress, Internet-Draft, draft-km-intarea-ocn-00, 2 July 2022, <https://datatracker.ietf.org/doc/html/draft-km-intarea-ocn-00>.

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

2016.7479438, August 2016, <https://doi.org/10.1109/ieeestd.2016.7479438>.

[VIRT-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>.

Authors' Addresses

Kiran Makhijani
Futurewei

Email: kiran.ietf@gmail.com

Tooba Faisal
King's College London

Email: tooba.hashmi@gmail.com

Richard Li
Futurewei

Email: richard.li@futurewei.com

Cedric Westphal
Futurewei

Email: cedric.westphal@futurewei.com