Internet Area Working Group
Internet-Draft
Intended status: Informational
Expires: 3 January 2023

T. Faisal
King's College London
D. Lopez
Telefonica I+D
J. Ordóñez-Lucena
Telefonica
K. Makhijani
Futurewei
2 July 2022

Problem Statement and Requirements for the Operation and Control Networks (OCNs)
draft-tf-ocn-ps-00

Abstract

The emergence of applications based on machine-to-machine communications require control systems to be extended beyond their closed environments. Specifically, autonomous systems that bring about physical and mechanical changes to an environment, heavily rely on their remote operations and control.

This document provides an overview of the issues associated with the communications in the control systems to support network-based operations in a generic manner at any-scale environments.

The term Operations and Control networks (OCN) is used to describe the common characteristics emerging from the requirements for such control systems.

The OCNs are technology-agnostic concept. This document aims to discuss the requirements for establishing common interfaces and functions.

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

Recently, we have witnessed an inflated number of devices and diversity in applications. With the advent of 5G and soon-to-be-reality 6G, several use cases such as autonomous and remote-driving vehicles, smart grids and smart healthcare are being introduced and demonstrated.

This introduces new challenges for the network service providers. For example, some applications (e.g., V2X) require stringent service quality (specific latency, bandwidth at visual quality and extreme reliability) whereas in traditional applications, best-effort service would have sufficed (e.g., internet browsing for non-urgent emails).

Industrial applications will be both time-constrained and geographically-limited. This means that service quality requirement will need to be handled on case by case basis. For example, in the energy grid, when a transmission line outage disconnects a large industrial customer, it leads to a situation in which the total electricity generation exceeds the total electricity demand, and frequency rises which can lead to unstable power grid [NREL-ESI]. To respond quickly in sub-second time period, different components in the energy-grid must be continuously monitored in real-time so that the control center can take several actions instantaneously, such as timely change in the voltage transformer to avoid dangers to the equipment and personnel and even re-routing alternate power resource.

Geographically-limited means, that some of the areas will be more dense than others, and vise versa. If a service provider has promised a connection for a remote vehicle, for example, in that case, the connection guarantee would be required for complete journey of the car. Naturally, the car may pass through areas where the service provider may not have connectivity due to reasons such as less-demand, but they still have to provide connectivity to their customers, if they have agreed. Resource sharing arrangements may be already in place between the providers to fulfill the demands of their customers. It is the providers' responsibility to ensure that they can provide guaranteed service throughout the journey, and if they cannot, such limitations must be clearly communicated with the customer at the time of service agreement.

Another challenge with fast-moving devices (vehicles) is that they send their data (e.g., GPS locations and service information) to the control centre periodically. The controller will also send updated information, for example, route and roadwork data. The control

centre may be sitting on the edge, cloud or other remote location. If the connectivity between the vehicle and the control center is not stable and is not up to the minimum required level, the data cannot be delivered to/from the vehicle. The results of such malfunctioning can be catastrophic, for instance, accidents and wrong routes.

The biggest challenge is that the networks are now required to support the control systems to bring desired outcome by delivering operational instructions to machines and connected devices remotely.

In control system aware networks, promising and adhering to service guarantee is not trivial. They are prone to system level catastrophic failures due to violations in service guarantees, such as packet drop and jitter. This work explores ways to provide service guarantee such that under no circumstances QoS is affected.

The document discusses the issues in the connected control system scenarios observed in [FACTORY], [ENERGY-GRIDS], and [V2X-UC] and introduces a general reference model called Operations and Control Networks (OCN) for the support of control systems over any network. The details of OCN are covered in [MODEL].

2. Conventions and Definitions

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

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.

Frequency response:
the ability of the power system to stabilize and restore grid frequency following large, sudden mismatches between generation and load. It has always been an operational concern.[NREL-REPORT].

3. Issues and Concerns

In general-purpose network paradigm which is based on the fairness among different flows, mechanisms are designed to deliver as much traffic as possible across the networks. Packets flow through the medium and the fate of the packets is uncertain.

In contrast, in control networks, the performance metrics are required to be certain. Since the packets may be carrying extremely important control information such as managing a power surge in a smart grid, a packet drop can be catastrophic.

3.1. Diversity in Service Quality

The concern for service operators is to provide networks capable of delivering control-systems specific services and to have a better understanding of the control systems. They will also benefit from knowing what gaps exist and what technologies or tool sets are available.

Service operators can assess three possible categories for service quality as below:

* Best-Effort Connection -- traditional best-effort services will suffice for applications such as video streaming and web browsing.

* Bounded-Latency Connection -- These kind of network applications

will require specifc QoS metrics and beyond and below those metrics the applications will not accept. For example, remote surgery, in which an autonomous arm will require specific metrics such as speed and delay.

* Hard-Service Connection -- These kind of network applications will have minimum QoS requirements and any better QoS metrics provided to them will not cause any problem. For example, tele-surgery.

  Note: TODO: Lijun's comment: Those three service qualities should sometime match to the below guaranteed and non-guaranteed categories. Do you really only have three sub-categories? What about bounded-loss connection, bandwidth-guaranteed connection. It is also hard for me to understand what is hard-service connection. Do you mean better performance would not benefit more to those applications?

What separates control systems from other applications are the specific operational requirements on per transaction or on per request basis. In such applications the service quality required will be further diversified. For example, the customers for non-essential use cases can be allocated non-guaranteed service connection, and the control system applications will be given the guaranteed service.

3.2. Connected Sensors and Actuators

Industrial systems operate in specific conditions and therefore, are challenging to manage and operate. Requirements such as connectivity among devices vary from industry to industry. For example, an automobile plant may require lower latency for its robots dedicated for assembly than a solar farm sending its readings to a control center.

Another nuance in the Industry control systems relate to type of end-points and the type of traffic between the end-points. The data traffic essentially carry instructions that cause machines or equipments to move and do things within or at a specific time. Moreover, there is little to no context as a session between the two endpoints.

One end in such systems is a controlling entity and other two are the sensors and actuators. Both the actuators and sensors do not perform decision making tasks. The controller has those responsibilities.

The packets delivered from the controller are the actionable instructions to actuating device and largely fit into a single packet. Also, the data exchange is peer to peer between the controller and the field-device.

This forwards to challenge when a single sensor or actuator can essentially convey the outdated data to the controller, resulting in the wrong readings. Secondly, the IoTs applications themselves may have diverse QoS requirements. For example, robots working in automobile factory may have different QoS requirement than the robots working in a solar farm.

NOTE: I removed malfunctioning because network can not do anything if the endpoint is misbehaving.

3.3. Limitations and Complexities

3.3.1. High Precision Data Delivery

Large control systems, such as energy grid and V2X depend upon the data from the field devices. The data is essential for smooth operation of the field devices. If the data is somehow delayed, it will convey the wrong and useless information to the control system. It is important that the data generated by the field devices are timely and must contain the timestamp or some other notion of timing service to ensure the validity of the data.

3.3.2. Computational Abilities

Control systems would benefit from the use of sophisticated compute power. This allows them to build complex sequences of commands to co-ordinate between different machine operations. This creates a requirement to place controllers at the edge or in the cloud where advanced software techniques are feasible. However, field devices themselves are not involved in the decision making, thus requiring an interface from the edge/cloud controllers to the field devices.

3.3.3. Use of AI/ML Technologies

NOTE: Role of AI in prediction of supply-chain, maintenance planning.

Future control networks are required to be AI-enabled. Using prediction algorithms the control systems will be able to make predictions about the health and maintenance of the network.

Therefore, future control network systems must support AI/ML technologies to enable autonomous maintenance and operations tasks. For example, in a smart grid, thousands of devices will be installed. Using AI/ML algorithms the control centre should be able to predict the health of the devices and create alerts when the maintenance is due. Using AI algorithms, the control network should be able to order the required tools for maintenance without any delay and even before the system stopped working.

The use of AI in control systems leads to previously mentioned Section 3.3.2 capability. The output of AI models may request dynamic unplanned changes to the processes causing changes to traffic volume or latency sensitivities.

3.3.4. Cyber-Security Threats

Control networks such as energy grids are prone to cyber threats. These systems manage hundreds and thousands of field devices, controlled by a control system. Two main types of attacks are possible in the large networks such as energy grids:

* Passive Attacks: In these types of attacks adversary learn about the network through the data generated by the field devices. Typically, data is not changed or modified by the adversary in this situation and the motive of an adversary is merely to get the internal information of the system.

* Active Attacks: In Active Attacks, the adversary tempers (e.g., modify, replay) with data. The adversary, in this case, has some access to the devices that allows them to harm the system. For example, the adversary can send the incorrect readings to the control system believing the system is working well even if there are system errors. In another example, the adversary can make the field devices send large data bursts to the control system causing denial-of-service. Some examples of active attacks are man-in-the-middle attacks and flooding.

Since control systems are far more critical and changes in their behavior can potentially be catastrophic or large-scale outages. Therefore, every packet in control networks towards actuators/sensors should be verifiable and secured against either type of above mentioned attacks.

4. Motivation (Problem Statement)

Scenarios described in [FACTORY], [ENERGY-GRIDS], and [V2X-UC] are only representative scenarios, but they all require automation and autonomous decision making and execution of control logic over the networks with special capabilities to produce desired outcomes and results. Such a well-defined special-purpose network can minimize need for proprietary approaches (which is the current norm), integrate heterogeneous controlled environments into a single application domain to leverage cloud-native technologies.

These special-purpose networks are referred to as Operations and Control Network's (OCN). The OCNs need to support capabilities and functions that closely emulate process-automation. For example, closed-control of feedback loops, open-control loops, instructions to machines, collecting sampled and absolute data.

Furthermore, Modern paradigms such as distributed ledger technology (DLT) may be leveraged on top of the OCNs to validate success of operations performed. DLTs will enable automation, transparency and accountability among different stakeholders in industrial systems to improve overall security in control systems. In a typical industrial network, several key players are likely to be involved, for example, vendors and service providers. Using smart contracts (a distributed ledger-based software code), the agreements and dealings between these stakeholders are recorded and executed automatically.

5. Requirements

The requirements mentioned emerge from the study of differences between the general-purpose networking paradigm and OCN. Each of the characteristic in control system lead to a requirement in the network.

Similar to the mechanisms that Internet technologies deploy to support a large variety of applications, OCNs will be required to support control loops with different type of message delivery constraints. This may include latency as low as 5ms (e.g. in substations, energy grid), 10 ms in factory floors.

The requirements mentioned below considers communication between the three key components - sensors, actuators and their controllers.

5.1. Control Loops

The performance of a control system is characterized by the success of associated one or more requests. These requests are sensitive to when the command actually executes, in effect the expectation from the networks is to be aware of the latency constraints.

The process automation requires that several instructions are executed in order. Not all field devices are capable of remembering past actions. For example, an actuator upon receiving a function code will mmediately perform correspondig action. Therefore, 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, therefore, getting the response back in specified time is required, leading to knowledge of timing.

5.2. Traffic distribution

* Well-engineered behavior: Control systems are well-engineered. Each OCN application knows how, when and where the commands will be executed, including the sequence which will be followed (under normal conditions) and the periodicity of sensors. Random spikes in traffic will generally be characterized as an abnormal behavior. The networks are required to observe and report such anomalies by recognizing unexpected traffic changes.

* Ordering: As mentioned in Section 5.1 out of delivery not tolerated and at the same time, field-devices are not equipped to run sophisticated transport protocols. Therefore, networks are required to support ordering.

* Per-packet expectations: unlike internet applications where performance is managed on the flow basis. the instructions for the most cases are self-contained therefore, the flow-based techniques of policing, buffering and identification do not apply.

* Congestion Control: While congestion can be tolerated in general-

purpose networks on end nodes, OCN packets can not be delayed. Therefore, alternatives to priority based and end-point based scheduling and delivery methods are necessary.

5.3. High Precision Requirements

Not only that different scenarios have different constraints, even commands with in an application have different time requirements. Moreover, different types of latencies are feasible for different commands such as certain actions must happen at a clock time, or in a bounded time , or before a specific time, or periodically.

In the internet application, with human in the loop tolerance is much higher with buffers on endpoints can be upto 100ms depending on the application. Whereas per scenarios in Energy grid [ENERGY-GRIDS] latency ranges between 5 to 30 ms.

5.4. Safety and Reliability

TODO: how do you guarantee that each operation has correct execution. TODO: what are requirements of safety.

Industrial systems depend on several components: field devices, communication channel and control center all contribute to the operations. If any of these components are not performing correctly, the whole system can be compromised.

The control center must get the correct data from the field devices and vise versa. This includes that the field devices are performing in the right conditions.

Industrial systems must ensure that all the components (i.e., field devices, communication channel and the control center) within the control network are secured and sending only reliable data. If the data is tempered somehow, or the devices are not performing as expected, the fault must be isolated without any delay.

Note: this section can be improved.

5.5. Communication model

In Operation and Control Networks, choosing a right communication model is important. For example, a smart grid OCN model can help to prevent the energy waste and store surplus energy in the distributed storage nodes.

Typically, field devices (sensors and actuators) may send the data to the controller in two ways:

* Point-to-Point (unidirectional): a field device (e.g., car sensor, current transformer actuator) is connected to the controller directly and sending/receiving data directly.

* Relayed communication: a field devices does not have direct connectivity to/from the controller and using intermediate devices for the communication.

Operation and Control network advocates the point-to-point communication between a field device and the controller, at least logically so that the requirements between them are explicit and the same with or without the networks.

5.6. Connectivity Architecture

The connectivity is hierarchical as covered in [PLC-VIRT]. Data flows in particular centralized manner using ICA model. In this document the need for a distributed architecture and virtualization s also discussed.

The high level representative communication model is depicted in Figure 1.

```
              <-- Applications -->
                ================
                  /            \
       +------------+       +-------------+
       | controller|        | controller |
       |     A      |       |     N       |
```

```
            +-----------+      +-------------+
             /      \                |
            /        \               |
           /          \              |
        +-------+   +----------+   +----------+
        |sensor|    | actuator|    | actuator|
        | FD1  |    |  FD2     |   |  FDNx    |
        +-------+   +----------+   +----------+
```

Figure 1: Generalised communication model of OCN

Control systems have specific data flow. A field/remote device sends/receives both continuous (e.g., temperature readings) and bursty data (e.g., camera's visual feeds) to/from the controller. For example, an autonomous vehicle will be in communication with the controller to get the weather and the route data Figure 1. On the other hand the vehicle will also be sending the field information (e.g., GPS info) to the controller.

Field devices such as sensors and actuators have no computational power. This means if the connection with the control centre cannot be established between a device and the control centre they cannot make routing decisions. Consequently, the device cannot send/receive

important control information. To that end, all the devices must have connectivity among themselves to act as a rely on other devices, in such a situations.

Operational and control networks (OCN) should not allow packet loss, for some commands. Therefore, an important consideration here is that the OCNs should provide resources such as bandwidth, preferred scheduling or alternate path to accommodate for the traffic in the region.

5.7. Accountability

Operation and control networks are delay intolerant and communication channels may suffer from errors causing packet loss and jitter. This means that if the QoS is affected due to any reason, the original cause must be known and the responsible party must be held accountable. The reason due QoS change does not need to be the operator or service provider. It is also possible that the devices or the controller may malfunction. Therefore, accountability is of paramount requirement in OCN.

To this end, smart contracts [SMART] like solutions may be beneficial in OCN. Smart contracts are auto-executable software codes that executes on some certain predefined conditions. All the time-sensitive and delay-intolerant applications in OCN record the data through smart contracts. Penalty clauses in smart contracts will get executed and the responsible party will be held accountable.

TODO: Do we need details how the blockchain and smart contracts will be part of OCN?

In the example of an energy grid (Figure 2) data about the availability of bulk energy will be passed on to the transmission grid. Similarly the usage information will be passed on to the distribution center and transmission to know the exact usage of the energy.

```
+----------------+   +----------------+   +--------------+  +-------+
|                |   |                |   |              |  |Smart  |
|Bulk Generation |----  Transmission  |---| Distribution |--|Meter  |
+----------------+   +----------------+   +--------------+  +-------+
```

Figure 2

The transmission model is generally in peer-to-peer, that is, a control center is in communication with the field device and vise versa. The high level communication model is depicted in Figure 1.

Industrial system operations are based on service delivery. The field-devices send the field data to the controller. The controller uses this data to make decisions such as temperature increase/decrease in a factory or changing engine fluid levels. This data is also sent to the control centre which uses this information to make long-term decisions such as keeping track of production costs.

If this data is corrupted or damaged due to any (malicious or non-malicious) reasons, the whole chain of decisions can be affected. Therefore, the data sent by the field-devices must be accurate. If for any reason the data is not accurate, the exact reason for the inaccuracy and the party at fault should be identified.

Similarly, in OCN, applications execute operations on the field-devices to extract data through northbound interfaces. The data from the field devices may have sensitive information such as the vehicle's location, if this information is compromised by the application, the privacy of the vehicle can be jeopardised.

To this end, OCN may enable accountability through smart contracts. The applications which require extracting data from field-devices must run a smart contract to request access to the field-devices. In such a way the party, in fact accessing the field-devices will have to be recorded by the smart contract and will be held accountable, if any wrongdoing happens.

6. State of the Art

There have been several mechanisms to provide network support for control systems, a large number of them being proprietary approaches. In this section we discuss a few prominent ones.

Note: TODO - comprehensive gaps

Original communication technologies are field bus technologies. They achieve guarantees associated with time by using serial bus protocols. Over last several decades of industry automation, many different serial bus protocols have been designed to address different use cases. The options used to harmonize these protocols are designed from the application perspective at a high layer. The issues concerning time-requirements, safety, reliability are not seamlessly integrated. see [ADDRESS] for more details.

Even as transition to Ethernet is taking place, there is no common mechanism. There are real-time Ethernet, Profinet and TSN based approaches available. Time-Sensitive Networking standard provides guarantees of time in network services and also methods to mitigate packet losses. Due to their property of determinism, they are ideal

for control systems. In spite of their origins and popularity in Ethernet, an obvious challenge is the inter-connection of different TSNs, since as the scale and geographical expansion of use cases occur, mechanisms will be necessary to connect two islands of TSNs.

In this regard, OCN maybe a TSN or a network that interconnects two TSNs while preserving all its properties.

DETNET [RFC9023] has been actively looking into providing TSN type services in the network layer. The DetNet provides congestion and service protection along the path of a DetNet flow [RFC9016]. The DetNet flows provide bounded latency, low jitter and low packet loss and in-order delivery [DETNET-PRIMER]. It addresses requirements for scaling and distance using layer 3 networks. Detnet provides a network that could fulfill the control system requirements to an extent. Several control systems are not flow-centric due to command response structure. Each request is self-contained and not necessarily carry the notion of flows.

Besides, above examples, protocol development work related to end-to-end IP in constrained nodes over [IEEE802.15.4], ITU-T [G9959] Bluetooth Low Energy (BTLE) type of media is progressing. Protocols have been developed to support IPv6 over Low-Power Wireless Personal Area Networks (6LoWPAN) [RFC6282] [RFC6775] [RFC4944], CoAP ([RFC7252]). These have been involved with the handling of constrained, low bandwidth, low memory, battery-powered devices. A large portion of IoT work is focused on the consumer side devices to support IPv6 based stack over different media (primarily wireless or radio). In constrained networks, the time related functions are handled through message priorities, which may not always produce desired outcome. OCNs can be positioned to complement this work into corresponding network support and overcome the gaps in the Industrial IoT as discussed in [ADDRESS] and [PLC-VIRT].

The diversity of the above work and solutions demonstrates that a common model and a common interface is needed to make smooth transition from local operations to distributed multi-stakeholder use of control system.

7. Security Considerations

TODO Security

8. IANA Considerations

This document has no IANA actions.

9. References

9.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/rfc/rfc2119>.

[RFC4944] Montenegro, G., Kushalnagar, N., Hui, J., and D. Culler, "Transmission of IPv6 Packets over IEEE 802.15.4 Networks", RFC 4944, DOI 10.17487/RFC4944, September 2007, <https://www.rfc-editor.org/rfc/rfc4944>.

[RFC6282] Hui, J., Ed. and P. Thubert, "Compression Format for IPv6 Datagrams over IEEE 802.15.4-Based Networks", RFC 6282, DOI 10.17487/RFC6282, September 2011, <https://www.rfc-editor.org/rfc/rfc6282>.

[RFC6775] Shelby, Z., Ed., Chakrabarti, S., Nordmark, E., and C. Bormann, "Neighbor Discovery Optimization for IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs)", RFC 6775, DOI 10.17487/RFC6775, November 2012, <https://www.rfc-editor.org/rfc/rfc6775>.

[RFC7252] Shelby, Z., Hartke, K., and C. Bormann, "The Constrained Application Protocol (CoAP)", RFC 7252, DOI 10.17487/RFC7252, June 2014, <https://www.rfc-editor.org/rfc/rfc7252>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/rfc/rfc8174>.

[RFC9016] Varga, B., Farkas, J., Cummings, R., Jiang, Y., and D. Fedyk, "Flow and Service Information Model for Deterministic Networking (DetNet)", RFC 9016, DOI 10.17487/RFC9016, March 2021, <https://www.rfc-editor.org/rfc/rfc9016>.

[RFC9023] Varga, B., Ed., Farkas, J., Malis, A., and S. Bryant, "Deterministic Networking (DetNet) Data Plane: IP over IEEE 802.1 Time-Sensitive Networking (TSN)", RFC 9023, DOI 10.17487/RFC9023, June 2021, <https://www.rfc-editor.org/rfc/rfc9023>.

9.2. Informative References

[ADDRESS] Makhijani, K. and L. Dong, "Requirements and Scenarios for Industry Internet Addressing", Work in Progress, Internet-Draft, draft-km-industrial-internet-requirements-00, 10 June 2021, <https://datatracker.ietf.org/doc/html/draft-km-industrial-internet-requirements-00>.

[DETNET-PRIMER] Varga, B., Farkas, J., Fedyk, D., Berger, L., and D. Brungard, "The Quick and the Dead: The Rise of Deterministic Networks", January 2021, <https://www.comsoc.org/publications/ctn/quick-and-dead-rise-deterministic-networks>.

[ENERGY-GRIDS] "Networks for Operating Energy Grids", n.d., <https://kiranmak.github.io/draft-km-energygrid>.

[FACTORY] "https://kiranmak.github.io/draft-iotops-iiot-frwk", n.d., <TODO Add smart-factory Networks - Use case>.

[G9959] "Short range narrow-band digital radiocommunication transceivers - PHY, MAC, SAR and LLC layer specifications. ITU-T Recommendation G.9959", January 2015, <http://www.itu.int/rec/T-REC-G.9959>.

[IEEE802.15.4] "IEEE Standard for Low-Rate Wireless Networks", IEEE standard, DOI 10.1109/ieeestd.2016.7460875, n.d., <https://doi.org/10.1109/ieeestd.2016.7460875>.

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

[NREL-ESI] "Transient and Dynamic Stability Analysis", n.d., <https://www.nrel.gov/grid/transient-dynamic-stability.html>.

[NREL-REPORT] Miller, N.W., Shao, M., Pajic, S., D'Aquila, R., and K.

Clark, "Western Wind and Solar Integration Study Phase 3 – Frequency Response and Transient Stability: Executive Summary", January 2014, <https://www.nrel.gov/docs/fy15osti/62906-ES.pdf>.

[PLC-VIRT] 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>.

[SMART] Faisal, T., Maesa, D. D. F., Sastry, N., Mangiante, S., and ACM, "AJIT", DOI 10.1145/3411043.3412506, <http://dx.doi.org/10.1145/3411043.3412506>.

[V2X-UC] 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>.

Acknowledgments

TODO acknowledge.

Authors' Addresses

Tooba Faisal
King's College London
Email: tooba.hashmi@gmail.com

Diego Lopez
Telefonica I+D
Email: diego.r.lopez@telefonica.com

José A. Ordóñez Lucena

Telefonica
Ronda de la Comunicacion, s/n Sur-3 building, 3rd floor
Madrid
Spain
Email: joseantonio.ordonezlucena@telefonica.com

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