Harmonizing IoT Nodes in the Multi-tier Computational Model for Integrated Distribution Network Operations

Jonatas Boas Leite[1], *Member*, *IEEE*
[1]*Dep. of Electrical Engineering*
São Paulo State University - UNESP
Ilha Solteira - SP, Brasil
jb.leite@unesp.br

Mladen Kezunovic[2], Life *Fellow*, *IEEE*
[2]*Dep. of Electrical and Computer Engineering*
Texas A&M University
College Station - TX, USA
kezunov@ece.tamu.edu

***Abstract*—In the information era, microprocessor-based devices are being incorporated into human environment facilitating the human-machine relationship. Recently released credit card-sized computers are being used in internet of things (IoT) platforms originated from ubiquitous computing concepts. In the modern power system, ubiquitous computing systems can be configured to facilitate the transfer of energy by supporting various smart grid applications at the grid edge. Using such distributed computational resources is not trivial considering that the traditional power system energy management technology is mostly centralized. The use of the IoT technology requires interfacing of the distributed computational resources with the legacy centralized resources where microprocessor-based IoT nodes are interfaced to the advanced distribution management system and perform the distribution automation functions. This paper demonstrates how such devices are modeled by harmonizing IEC 61970/61968 and 61850 standards over a multi-tier computational model. The performed tests analyze the message flow of the fully automated procedures for fault location, isolation and service restoration applications.**

***Index Terms*—Advanced Distribution Management System, Distribution Network Operation, Internet of Things, Microprocessor-based IoT node.**

I. Introduction

The internet of things (IoT) concept comes from the ubiquitous computing initially envisioned by Weiser, 1991 that realized the intense integration among computers and natural human environment allowing the computers to be an indispensable background [1]. Around thirty years later, the mobile phone in hands of great portion of Earth's population provides increasing amounts of computing, sensing and communication capabilities, representing the most successful example of ubiquitous system. The cellular communication technology has also contributed to the implementation of smart grid applications, which eventually led to the use of IoT [2].

The IoT technology has been applied in several industrial sectors such as retail, healthcare, transportation, etc. [3]. In the energy management sector, for instance, home energy management system (HEMS) is optimizing the residential energy consumption and production by combining software tools, home-area network and energy sensors [4]. The energy management system (EMS) is integrating advanced metering, information technology (IT) and operational technology (OT) to allow the real-time, or near real-time data feeds to a wide range of equipment to reduce operating costs and increase reliability and productivity [5]. Moving the SCADA (supervisory control and data acquisition) to the cloud may lead to potential savings due to reduced setup time and technical staff to manage software and hardware [6].

The centralization through cloud computing provides consolidated resources and management but, at the same time, has weakness because limited communication capabilities with the devices near the process environment. Multi-tier computing networks can overcome these challenges [7]. In [8], the distribution automation is achieved by an IoT based SCADA integrated with fog computing as bridge between IoT node devices and the cloud. The distribution automation is divided in three sensing areas: smart meters; feeder sensors; and intelligent electronic devices (IEDs), using 3G/4G/5G and 6LowPAN communications. The use of plug-and-play equipment over cloud-based SCADA should lead to the implementation of smart grid applications, like self-healing schemes, as ubiquitous system. Some challenges are yet to be overcome, for example, the communication protocol running in the control center is different from the ones used in the substation and/or feeder automation [9].

The IEC standard 61850 covers the general communication to and from IEDs inside and outside of substations. The IEC common information model (CIM), which is described in a set of three standards, namely IEC 61970, 61968, and 62325, provides data model for the energy management system (EMS). Both 61850 and CIM are essential for smart grid deployment where the connections between the CIM, utilized in EMS, and IEC 61850, primarily utilized in substations, are established [10]. This benefits control center applications by facilitating access to IEC 61850 model and data items through the CIM. The models from CIM and IEC 61850 can be integrated with the domain specific proprietary models and, by deploying microgrid control system solution, the abstract models can be

This work was fully supported by the grant number "2019/07436-5" and "2015/21972-6" funded by the São Paulo Research Foundation.

communicated between nodes to support the plug-and-play ability of the controllers [11].

The contribution of this paper includes the harmonization solution for the interaction between CIM and IEC 61850 to enable IoT capabilities in smart grid applications. The modeling concept shows how the IoT-based distribution network operation utilizing logical models over more semantic languages makes autonomous algorithms feasible. The concept illustrates how the system architecture with IoT node devices dispersed along the distribution network must be implemented to take advantage of timing measurements on the fully automated procedures of the fault location, isolation and service restoration operation (FLISR), or self-healing.

II. Interfacing IoT Nodes in Smart Grids

The ubiquitous system and open hardware platform provide more flexibility when implementing smart grid applications. The cybersecurity and interoperability arise as an imminent challenge [12]. The use of IoT system standards with multi-tier computing model is a way to overcome these challenges.

A. Integrated Environment of Network Operations

The integrated environment is supported by IEC 61850 and IEC 61970/61968 standards that are recognized as essential resources in the integration of distribution network operations and smart grid realization [13]. In this paper, a step further is made to advance the interoperability between the utility datacenter services with near-to-energy-process devices by deploying the IoT node device model in the integrated environment of network operation, as depicted in Fig. 1.

The environment with SCADA, outage management system (OMS) and distribution management system (DMS) integrated as a network operation service, i.e., a web service that exchanges information using the enterprise service bus (ESB), depends on the harmonization solution between CIM and IEC 61850. The direct data exchange with ESB involves standardized interfaces and shaping the message structure in order to be CIM compliant. ESB messages are constructed using XML scheme (XSD) through defined information exchange by the standardized interfaces. The harmonization between CIM and IEC 61850 should thus allow the direct exchange of data with standardized interfaces via the IoT communication protocol.

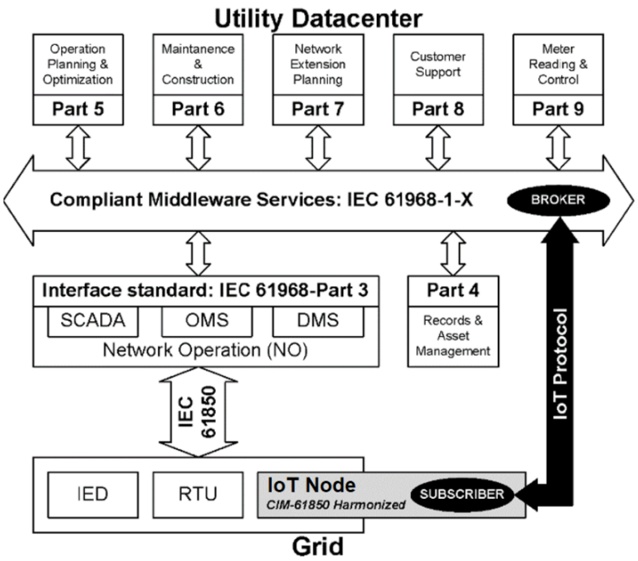


Fig. 1. Harmonized IoT node device in the distribution system.

B. MQTT Protocol and Broker Service

MQTT is a broker-based protocol. The MQTT broker, also commonly referred as a server, can be hosted locally or through a cloud-based service. In the broker system, a publisher posts a message to the broker which then passes that message on to any client subscribed to the topic specified by the publisher. These topics can be narrowed down in scope so that a user can be subscribed to a specific subtopic. Figure 2 shows a simple illustration of this publish/subscribe model. In a real-world scenario with IoT node device scattered across heterogeneous networks, the advanced DMS (ADMS) should at least know the master resource identifier (`mRID`) or name of the IoT node device to which it is sending a message. When IoT node devices are organized in hierarchical groupings, this messaging design might be more useful.

Topic management with MQTT is relatively simple at its core but allows for greater customization if desired. If a publisher sends a message for a topic that has no current subscribers, the broker will simply discard the information received unless the publisher has specified that the topic should be retained. For example, in the simplified diagram in Fig. 2, if the publisher sent out its first message for `iotND/REQUEST/Reading/Created` before there were any subscribers present, then this message would only ever be seen if the publisher had notified the broker that the message is to be retained. If subscribers to the topic `iotND/REQUEST/Reading/Created` connect to the broker after this message had been sent by the publisher, and if the message is set to be retained, then each subscriber should receive this message upon subscribing to the topic. This feature can be used in a situation where subscribers need the most recent value for created readings without having to wait for the publisher to push a new value.

Once the MQTT protocol envelops the IEC 61968-100 based messages, the IoT node device should be CIM-IEC 61850 harmonized, i.e. fully understandable by the utility datacenter.

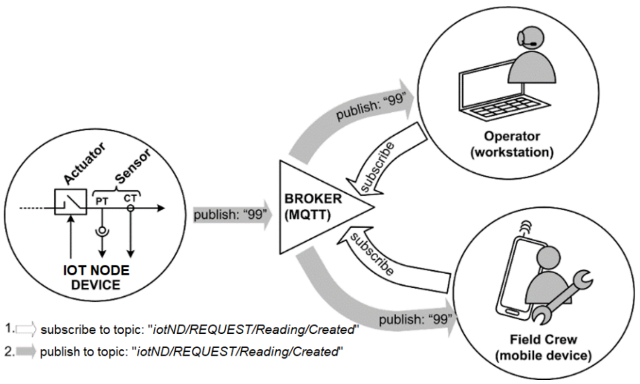

Actuator
Sensor
PT
CT
IOT NODE DEVICE
publish: "99"
BROKER (MQTT)
publish: "99"
subscribe
Operator (workstation)
subscribe
publish: "99"
Field Crew (mobile device)
1. subscribe to topic: "iotND/REQUEST/Reading/Created"
2. publish to topic: "iotND/REQUEST/Reading/Created"

Fig. 3. Publishing/subscribing message system over MQTT protocol.

C. Multi-tier Computational Model

Indeed, MQTT is recognized as a most suitable protocol for IoT platforms with high reliability, secure multicast communications and persistent messages [14]. MQTT broker resides, typically, in the cloud. Although cloud computing addresses major needs of IoT systems, such as location awareness, mobility and geo-distribution, it fails in timely decision-making process as required by power industry. Only cloud computing is not enough to support ubiquitous systems because of hard time-delay restrictions, intermittent network connectivity and restricted communication bandwidth [15].

Multi-tier computing overcomes these issues by introducing an intermediate layer between cloud computing infrastructure and IoT node devices bridging application in the cloud and the edge. The multi-tier computation model in [16] deploys MQTT protocol into three layers, as detailed in Fig. 3. The layer one hosts the IoT node devices near the power grid, or energy process. They enable to run MQTT client instances. In the second layer, there are remote brokers that assist the main broker in the cloud computing. The layer three, thus, is the main MQTT broker.

D. Harmonized IoT Node

IEC 61850 and the CIM standards specify structures and mechanisms for accessing power utility data. The IEC 61850 models are concentrated on the functions that can be seen and controlled, but not on how they work (what the algorithms are). The CIM standards also include a set of application neutral services, a set of XML messages (generic service payloads) that are used to exchange CIM data. Comparing the two, it can see a similar document structure [17]. These similarities support the use of a harmonized model that extends IEC 61970 CIM with new 61850 packages where technological profiles are the most important standard structure to implement an IoT node device.

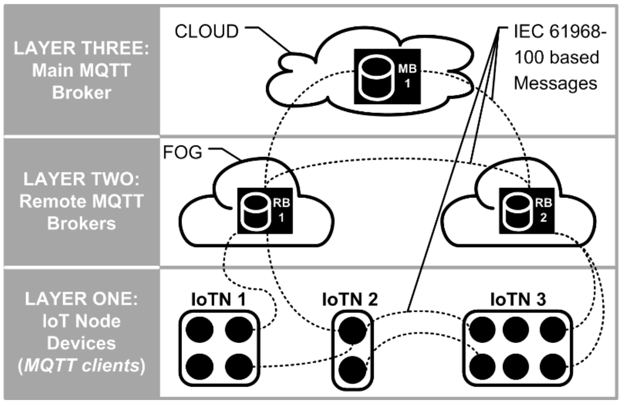

LAYER THREE: Main MQTT Broker
LAYER TWO: Remote MQTT Brokers
LAYER ONE: IoT Node Devices (MQTT clients)
CLOUD
FOG
MB 1
RB 1
RB 2
IEC 61968-100 based Messages
IoTN 1
IoTN 2
IoTN 3

Fig. 3. Connection of IoT node devices into multi-tier computational model with IEC 61968-100 based messages.

Typically, a CIM profile is a subset of the more general model. CIM objects, to be interchanged, must be available and have the same interpretation at both sides of the communication link. As CIM has plenty of optional features, both sides must have an agreement about the options to be used. Thus, an object containing the proposed class `iotNodeDevice` (see Fig. 4) could have all the attributes that appear in the class definition, while the other side object, none of them. Both objects comply with the definition of `iotNodeDevice` because the multiplicity of the attributes is zero or one, [0 or 1].

In Fig. 4, the IoT node device profile is built through the Enterprise Architect (EA®) software together with a harmonized model package, TC57CIM, using the unified model language (UML). The proposed IoT node device profile has classes from the `IEC61850::` package such as `LNClass`, `LNinst`, `LNode` and `LogicalDevice`. The package `Collections::`, from IEC 61850 scope, has the class `61850GroupTypeWithData` that is associated with the class `MeasurementValue` of the `Meas::` package from the IEC61970

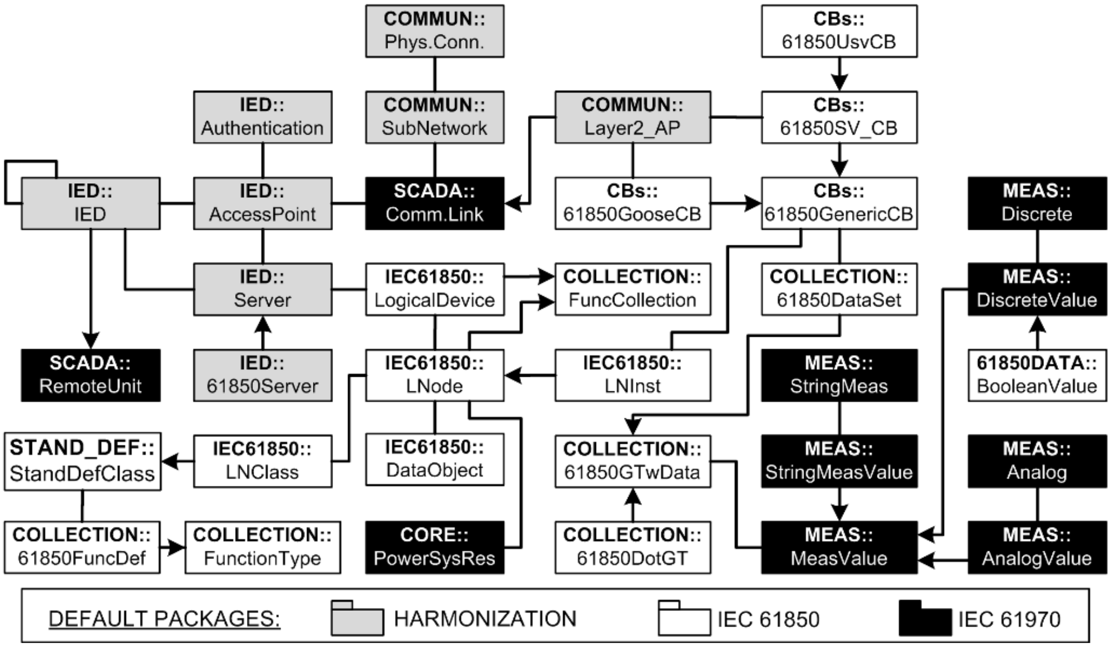


Fig. 4. Abstract modeling of the IoT node device in UML.

scope, for example. The `StringMeasurementValue`, `AnalgueValue`, `BooleanValue` and `DisceteValue` provide the abstract modeling of the functional points for monitoring and controlling the IoT Node device. In the harmonization scope, the `IED::` and `Communication::` packages provide classes comprising the models of the access points and communication interfaces to exchange information with the utility data center and/or other IoT Node devices.

III. Performance Assessment Results

The IoT node device abstract model was evaluated in hardware-in-the-loop test simulation environment [18] by sniffing the standardized messages. The employed single board computer (SBC) was the Raspberry Pi 3® under Windows 10 IoT Core. In this way, the abstract model was implemented using the C-Sharp (C#) programming language.

A. Hardware-In-The-Loop Test Setup

In Fig. 5, the stand-alone merging unit emulator collects current and voltage measurements from the power distribution network simulator (EDSIM) as described in [19] and sends this information to the IoT node device using sample values (SV) standardized by IEC 61850-9-2, once the IoT node device is not connected to the real-world electricity grid. After processing these measurements, the IoT node device can act under the simulated distribution system by sending GOOSE commands, instead of its actuation to the circuit breaker as in real-world power grid. In addition to work described in [18], the operator can now act on the IoT node device using standardized messages through the communication server that supports IoT platform subscribers by hosting the MQTT broker.

The communication server has two network adapters: one to private network connections including utility data center services, and another for the "public" network with IoT node devices near the electricity network energy exchange process. A firewall to safeguard the private network can then be hosted in the communication server, as well.

From a real-world perspective, this test setup environment should assist the operator by providing the event and security management system that must enable viewing of events in geographical information system (GIS) applications. Although the web application and database server also receive IEC 61968-100 messages, they are out the scope of the performed experiment where the functionalities of the IoT node device are checked as well as some standardized messages involved in an automatic FLISR procedure.

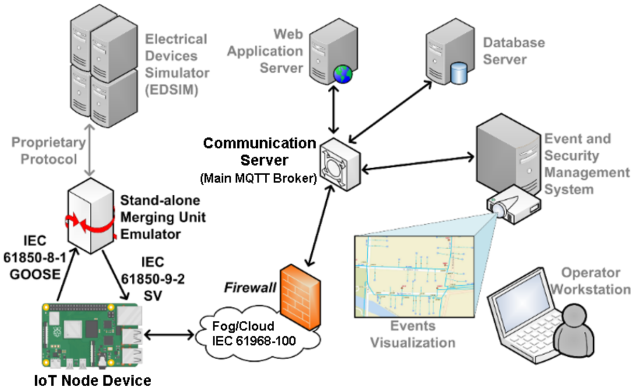


Fig. 6. Hardware-in-the-loop setup for validation experiments.

B. CIM-IEC 61850 Harmonized Messages

The evaluation of the message exchange through the MQTT protocol is done considering the automatic FLISR, i.e., the message sequence of the FLISR procedure for SCADA-detected outage and SCADA switching, as defined in [20]. This flow of information from FLISR considers a self-healing network, with the monitoring and control of the system provided by SCADA and automatic outage response directed by the fault management function of a DMS. The sequence diagram in Fig. 6 illustrates the message flow. Network control (NO-CTL), or SCADA, initiates this procedure when it detects an unexpected change in the state of a protection device and informs network operations (NO-NMON) of the unexpected event. Switching plans to isolate the fault and restore power are subsequently requested upon notification of the incident. NO-NMON must then direct NO-CLT to execute each step of the selected switching plan. The NO-CLT must inform the point of operation through standardized messages to an IoT Node device that performs control of switching equipment, such as a circuit breaker.

To perform the switching operation, first, the NO-CLT sends a request message to the IoT node device asking the creation of the `iotNodeDeviceControl` in order to change a `BooleanValue`. Figure 7 presents the Wireshark® capture analysis in the request message of the NO-CLT service at the ADMS application. In Fig. 9, the MQTT brokers are transparent but, as it is established in the multi-tier computational model in Fig. 3, every exchanged message out the network operation is sent to the ESB with the broker service. The broker receives the request message in the private network interface and, after 0.9 ms, sends it again to the public network to all IoT node devices subscribing to the topic. The request message has three parts: `<Header>`, `<Request>` and `<Payload>`. The last part informs the controlled point to be operated through the attribute `pathName` of the class `BooleanValue`.

The request message arrives at IoT node device that checks the ID and, when it is confirmed, the Control Model is executed to operate the Boolean value. The IoT node device commands

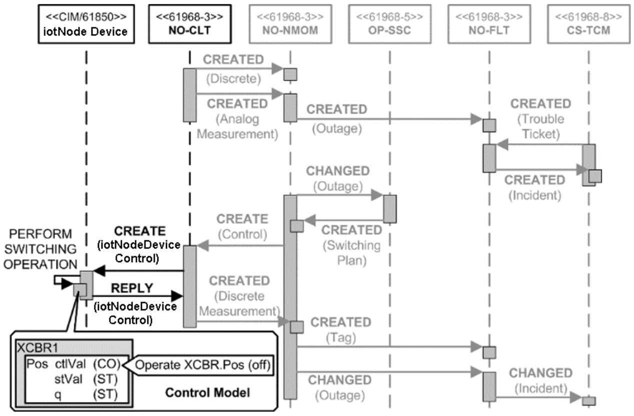
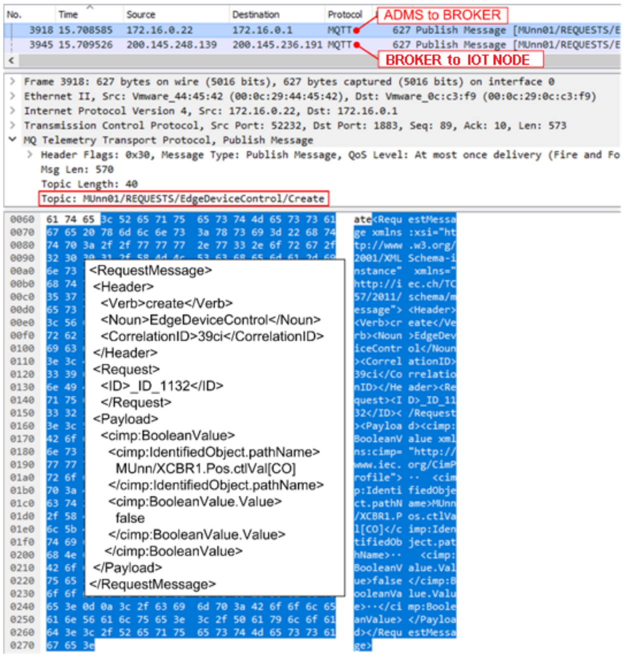


Fig. 6. Message flow for automatic FLISR with SCADA detection and switching.



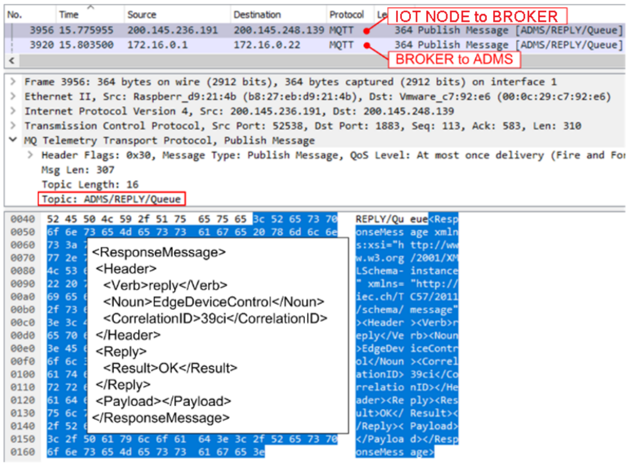
```
No.   Time       Source          Destination     Protocol
 3918 15.708585  172.16.0.22     172.16.0.1      MQTT      627 Publish Message [MUnn01/REQUESTS/E
 3945 15.709526  200.145.248.139 200.145.236.191 MQTT      627 Publish Message [MUnn01/REQUESTS/E

> Frame 3918: 627 bytes on wire (5016 bits), 627 bytes captured (5016 bits) on interface 0
> Ethernet II, Src: Vmware_44:45:42 (00:0c:29:44:45:42), Dst: Vmware_0c:c3:f9 (00:0c:29:0c:c3:f9)
> Internet Protocol Version 4, Src: 172.16.0.22, Dst: 172.16.0.1
> Transmission Control Protocol, Src Port: 52232, Dst Port: 1883, Seq: 89, Ack: 10, Len: 573
v MQ Telemetry Transport Protocol, Publish Message
  > Header Flags: 0x30, Message Type: Publish Message, QoS Level: At most once delivery (Fire and Fo
    Msg Len: 570
    Topic Length: 40
    Topic: MUnn01/REQUESTS/EdgeDeviceControl/Create

0060  61 74 65 3c 52 65 71 75  65 73 74 4d 65 73 73 61   ate<Requ estMessa
0070  67 65 20 78 6d 6c 6e 73  3a 78 73 69 3d 22 68 74   ge xmlns :xsi="ht
0080  74 70 3a 2f 2f 77 77 77  2e 77 33 2e 6f 72 67 2f   tp://www .w3.org/
0090  32 30 30 31 2f 58 4d 4c  53 63 68 65 6d 61 2d 69   2001/XML Schema-i
00a0  6e 73                                              nstance"  xmlns="
00b0  68 74                                              http://i ec.ch/TC
00c0  35 37                                              57/2011/ schema/m
00d0  65 73                                              essage"> <Header>
00e0  3c 56                                              <Verb>cr eate</Ve
00f0  72 62                                              rb><Noun >EdgeDev
0100  69 63                                              iceContr ol</Noun
0110  3e 3c                                              ><Correl ationID>
0120  33 39                                              39ci</Co rrelatio
0130  6e 49                                              nID></He ader><Re
0140  71 75                                              quest><I D>_ID_11
0150  33 32                                              32</ID>< /Request
0160  3e 3c                                              ><Payloa d><cimp:
0170  42 6f                                              BooleanV alue xml
0180  6e 73                                              ns:cimp= "http://
0190  77 77                                              www.iec. org/CimP
01a0  72 6f                                              rofile"> ··  <cim
01b0  70 3a                                              p:Identi fiedObje
01c0  63 74                                              ct.pathN ame>MUnn
01d0  2f 58                                              /XCBR1.P os.ctlVa
01e0  6c 5b                                              l[CO]</c imp:Iden
01f0  74 69                                              tifiedOb ject.pat
0200  68 4e                                              hName>··   <cimp:
0210  42 6f                                              BooleanV alue.Val
0220  75 65                                              ue>false </cimp:B
0230  6f 6f                                              ooleanVa lue.Valu
0240  65 3e 0d 0a 3c 2f 63 69  6d 70 3a 42 6f 6f 6c 65   e>··</ci mp:Boole
0250  61 6e 56 61 6c 75 65 3e  3c 2f 50 61 79 6c 6f 61   anValue> </Payloa
0260  64 3e 3c 2f 52 65 71 75  65 73 74 4d 65 73 73 61   d></Requ estMessa
0270  67 65 3e                                           ge>
```

```
<RequestMessage>
 <Header>
   <Verb>create</Verb>
   <Noun>EdgeDeviceControl</Noun>
   <CorrelationID>39ci</CorrelationID>
 </Header>
 <Request>
   <ID>_ID_1132</ID>
   </Request>
 <Payload>
   <cimp:BooleanValue>
     <cimp:IdentifiedObject.pathName>
       MUnn/XCBR1.Pos.ctlVal[CO]
     </cimp:IdentifiedObject.pathName>
     <cimp:BooleanValue.Value>
       false
     </cimp:BooleanValue.Value>
    </cimp:BooleanValue>
 </Payload>
</RequestMessage>
```

Fig. 7. Wireshark® captures analysis in publishing/subscribing message system with IEC 61968-100 standardized request message.

directly the circuit breaker in real-world but, in the simulation environment, the IoT node device uses the GOOSE message to report the new status in the EDSIM.

The IoT node device sends a reply message to the NO-CLT service at the ADMS reporting the result of the `iotNodeDeviceControl` created in order to change a `BooleanValue`. Figure 8 displays the Wireshark® capture analysis in the reply message of the IoT node device. Before reaching the ADMS, the IoT node device message passes through the MQTT broker that sends this message to all subscribers of the topic `ADMS/REPLY/Queue`. Like the request message, the reply message is comprised by `<Header>`, `<Reply>` and `<Payload>`. In the header, the `<CorrelationID>` provides a mean to associate this arriving message with those one sent initially. The payload with `<Result> OK` indicates that the requested operation was successfully performed.



```
No.   Time       Source          Destination     Protocol Le
 3956 15.775955  200.145.236.191 200.145.248.139 MQTT      364 Publish Message [ADMS/REPLY/Queue]
 3920 15.803500  172.16.0.1      172.16.0.22     MQTT      364 Publish Message [ADMS/REPLY/Queue]

> Frame 3956: 364 bytes on wire (2912 bits), 364 bytes captured (2912 bits) on interface 1
> Ethernet II, Src: Raspberr_d9:21:4b (b8:27:eb:d9:21:4b), Dst: Vmware_c7:92:e6 (00:0c:29:c7:92:e6)
> Internet Protocol Version 4, Src: 200.145.236.191, Dst: 200.145.248.139
> Transmission Control Protocol, Src Port: 52538, Dst Port: 1883, Seq: 113, Ack: 583, Len: 310
v MQ Telemetry Transport Protocol, Publish Message
  > Header Flags: 0x30, Message Type: Publish Message, QoS Level: At most once delivery (Fire and For
    Msg Len: 307
    Topic Length: 16
    Topic: ADMS/REPLY/Queue

0040  52 45 50 4c 59 2f 51 75  65 75 65 3c 52 65 73 70   REPLY/Qu eue<Resp
0050  6f 6e 73 65 4d 65 73 73  61 67 65 20 78 6d 6c 6e   onseMess age xmln
0060  73 3a                                              s:xsi="h ttp://ww
0070  77 2e                                              w.w3.org /2001/XM
0080  4c 53                                              LSchema- instance
0090  22 20                                              " xmlns= "http://
00a0  69 65                                              iec.ch/T C57/2011
00b0  2f 73                                              /schema/ message"
00c0  3e 3c                                              ><Header ><Verb>r
00d0  65 70                                              eply</Ve rb><Noun
00e0  3e 45                                              >EdgeDev iceContr
00f0  6f 6c                                              ol</Noun ><Correl
0100  61 74                                              ationID> 39ci</Co
0110  72 72                                              rrelatio nID></He
0120  61 64                                              ader><Re ply><Res
0130  75 6c                                              ult>OK</ Result><
0140  2f 52                                              /Reply>< Payload>
0150  3c 2f 50 61 79 6c 6f 61  64 3e 3c 2f 52 65 73 70   </Payloa d></Resp
0160  6f 6e 73 65 4d 65 73 73  61 67 65 3e               onseMess age>
```

```
<ResponseMessage>
 <Header>
   <Verb>reply</Verb>
   <Noun>EdgeDeviceControl</Noun>
   <CorrelationID>39ci</CorrelationID>
 </Header>
 <Reply>
   <Result>OK</Result>
 </Reply>
 <Payload></Payload>
</ResponseMessage>
```

Fig. 8. Wireshark captures analysis in publishing/subscribing message system with IEC 61968-100 standardized request message.

IV. Concluding Remarks

The following are the paper findings:

- The IoT node device abstract model is designed as a CIM profile by using Enterprise Architect® software together with the harmonized model package;
- The evaluation of the IoT node device abstract model uses a hardware-in-the-loop test simulation environment by sniffing the sequence of messages that are exchanged between the grid and utility data center using standardized messages of IEC 61968-100 encapsulated by the MQTT protocol;
- The implementation of the CIM-IEC 61850 harmonized IoT node device facilitated by the MQTT protocol demonstrates the feasibility of decentralized distribution automation based on IoT devices.

References

[1] L. Oliveira, et al. “The computer for the 21st century: present security & privacy challenges” *J Internet Serv Appl*, v. 9, n. 24, pp. 1-25, 2018.

[2] Y. Saleem, et al. "Internet of Things-Aided Smart Grid: Technologies, Architectures, Applications, Prototypes, and Future Research Directions," *IEEE Access*, v. 7, pp. 62962-63003, 2019.

[3] D. McFarlane, “Industrial Internet of Things: Applying IoT in the Industrial Context,” from https://www.ifm.eng.cam.ac.uk/uploads/DIAL/ industrial-internet-of-things-report.pdf, May 9, 2022.

[4] S. Li, et al. "A Real-Time Electricity Scheduling for Residential Home Energy Management," *IEEE Internet Things J.*, v. 6, n. 2, pp. 2602-2611, 2019.

[5] N. Hossein Motlagh, et al. "Internet of Things (IoT) and the Energy Sector," *Energies*, v. 13, n. 2, pp. 1-27, 2020.

[6] F. A. Osman, et al. "Secured cloud SCADA system implementation for industrial applications," *Multimed Tools Appl*, 81, pp. 9989–10005, 2022.

[7] Y. Yang, et al. "Computing and Service Architecture for Intelligent IoT", *Intelligent IoT for the Digital World: Incorporating 5G Communications and Fog/Edge Computing Technologies*. USA: John Wiley & Sons, Ltd., pp. 61-96, 2021.

[8] R. J. Tom and S. Sankaranarayanan, "IoT based SCADA integrated with Fog for power distribution automation," *2017 12th CISTI*, pp. 1-4, 2017.

[9] J. Northcote-Green, R. G. Wilson, “Control and Automation of Electrical Power Distribution Systems”, United Kingdom: CRC Press, 2017.

[10] A. Schumilin, et al. "A Consistent View of the Smart Grid: Bridging the Gap between IEC CIM and IEC 61850," *2018 44th SEAA*, pp. 321-325, 2018.

[11] R. Belu, “Smart Grid Fundamentals: Energy Generation, Transmission and Distribution.” United States: CRC Press, p. 486, 2022.

[12] A. Gopstein, et al. "NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 4.0," *Special Publication (NIST SP), National Institute of Standards and Technology,* Gaithersburg, MD, May 9, 2022.

[13] J. -S. Kim, et al. "Microgrids platform: A design and implementation of common platform for seamless microgrids operation," *Electric Power Systems Research*, v. 167, pp. 21-38, 2019.

[14] R. Venanzi, et al. "MQTT-Driven Node Discovery for Integrated IoT-Fog Settings Revisited: The Impact of Advertiser Dynamicity," *2018 IEEE Symposium on Service-Oriented System Engineering (SOSE)*, pp. 31-39, 2018.

[15] Y. Yang, “Multi-tier computing networks for intelligent IoT,” *Nat Electron*, v. 2, pp. 4–5, 2019.

[16] M. Veeramanikandan, S. Sankaranarayanan, “Publish/subscribe based multi-tier edge computational model in Internet of Things for latency reduction”, *Journal of Parallel and Distributed Computing*, v. 127, 2019, pp. 18-27.

[17] T. Berry. "Introduction to IEC 62361-102 CIM-61850 harmonization," *25th International Conference on Electricity Distribution*, Madrid, Spain, pp. 1-5, 2019.

[18] C. Reiz and J. B. Leite, "Hardware-In-the-Loop Simulation to Test Advanced Automation Devices in Power Distribution Networks," *IEEE Transactions on Power Delivery*, v. 36, n. 4, pp. 2194-2203, Aug. 2021.

[19] J. B. Leite and J. R. S. Mantovani, “Development of a Smart Grid Simulation Environment, Part I: Project of the Electrical Devices Simulator”, *J. Control Autom. Electr. Syst.*, v. 26, n. 1, p.80, 2015.

[20] “IEC 61968-3: Application integration at electric utilities - System interfaces for distribution management - Part 3: Interface for network operations”, April, 2021.