INTEROP

PLUGFEST 2022

INTEROPERABILITY PLUGFEST

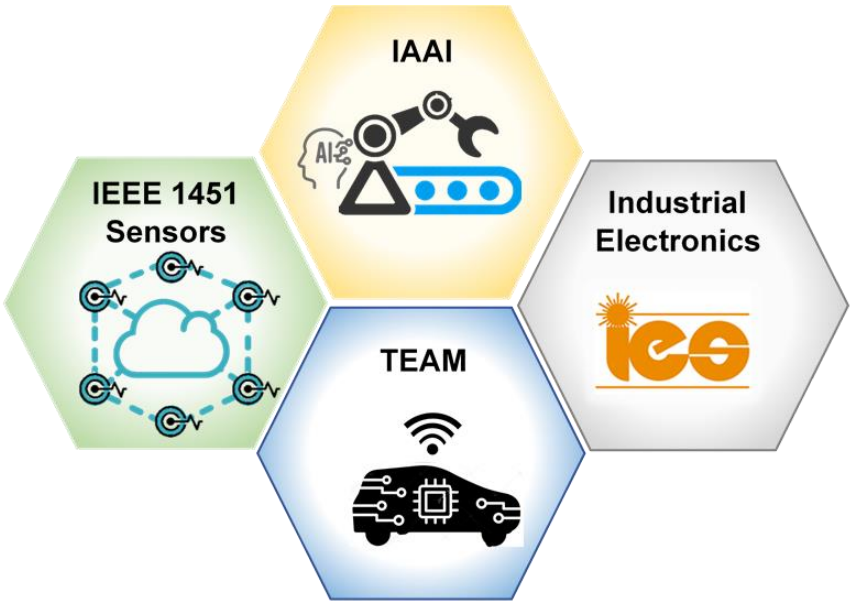
IEEE

SQUARE Brussels Meeting Centre
Brussels, Belgium

IES

INTEROP 2022

IES STANDARDS AND INTEROPERABILITY PLUGFEST



IEEE 1451 Sensors Standards Cluster

1. P1451.0
2. P1451.002
3. P1451.1.5
4. P1451.1.6
5. P1451.5.10 NB-IoT
6. P1451.99

Industrial Automation-Artificial Intelligence (IAAI) Cluster

1. P2668
2. P2992

Industrial Electronics Cluster

1. Smart Battery Gauge
2. P2023
3. Demo-Miami-Ohio
4. India CoE

Transportation Electrification & AutonoMous Vehicles (TEAM) Cluster

1. Automotive 1
2. Automotive 2

Industrial Electronics Society – IES Standards TC Standards Technical Committee

Table of Contents

WELCOME – INTEROP PLUGFEST 2022 3

About INTEROP 3

OBJECTIVES 4

Previous Editions 5

Testimonials from Previous Editions 5

INTEROP Demo Summaries 6

- *IEEE P21451-1-6 Time Synchronization* 7
- *IEEE P2992 – Data Expression, Exchange and Processing in Smart Agriculture* 9
- *Using Provisioning in IEEE P1451.99 to Assert Ownership of Information* 11
- *A New Architectural Approach for P1451.99 Binding to P1451.0: A First Proposal for P1451.99.0* 13
- *Semantic Interoperability in Transducer Management based on IEEE 1451* 15
- *Demonstration of IEEE P1451.5.X Smart Interfaces for Low Power Wide Area Networks* 17
- *IEEE P2668 Demonstration for INTEROP 2022* 19

PROGRAM ORGANIZERS:
Antonio Espirito-Santo
Allen Chen
Dietmar Bruckner

DEMO ORGANIZERS:
Kim Fung Tsang
Akshay Rathore (automotive)
Fei Gao (automotive)

PUBLICITY: V. Huang

ADVISORS: (outside of Stds TC)
Valeriy Vyatkin VP TA - IES
Peter Palensky Gen. Chair IECON
Victor Huang

STDS SESSION ORGANIZERS:
Allen Chen
Paulo Leitao

Contact IES STANDARDS TC Chair Cheng-Jen (Allen) Chen
Email: c.j.chen@ieee.org
Web: https://sites.google.com/view/iesstandardstc/about

WELCOME – INTEROP PLUGFEST 2022

The INTEROP Plugfest at IECON 2022 is the seventh edition of the IES Standards Committee's INTEROP Plugfest series. Continuing the successful annual series at IES flagship conferences, the 2022 IES INTEROP Plugfest is held at IECON 2022 in Brussels, Belgium, on October 17 – 20, 2022, and features ten (10) participants, representing diverse areas of practical and innovative technologies and applications, pre-standard processes aligning to IES fields of interest. Notable this year, as in last year, an additional Regional INTEROP Plugfest was held at IES ICIT 2022 conference in Shanghai, China, mainly due to the interest of the large concentration of high technology industry in the region (a similar regional Plugfest was held at ISIE 2021 in Kyoto in 2021).

We are honored to host our INTEROP participants at this practical interoperability event and showcase their plugfest demonstrations, and their efforts are memorably recorded in this brochure.

We thank you and your support to the IES Standards initiative, the IES Standards Technical Committee and the Industrial Electronics Society.

INTEROP Plugfest 2022 Organizers:

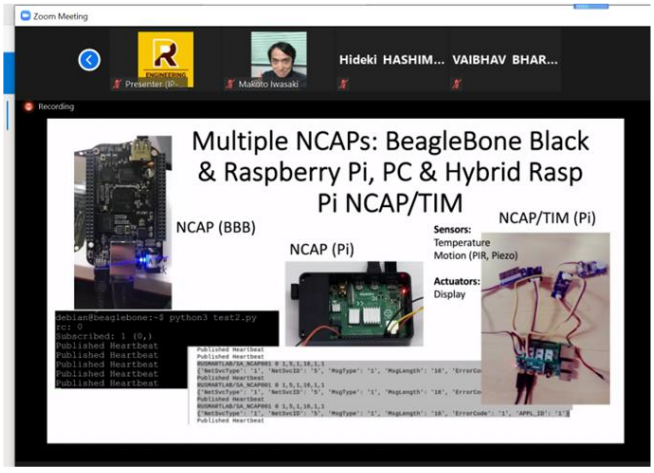
Antonio Espirito-Santo, Allen Chen, Dietmar Bruckner

ABOUT INTEROP

The INTEROP Plugfest was introduced by the Industrial Electronics Society's (IES) Standards Technical Committee in 2018 as an initiative for the Society's community to participate in a practical and demonstrative fashion in interoperability and potential standards compliance applications. This event is usually in conjunction with IES' yearly flagship conference, the Industrial Electronics Conference (IECON).

This is especially targeted to the society's academic and industry collaboration partners to come together in a physical neutral environment conducive to open technical discussions. The goal is to provide periodic gatherings of like-minded members to discuss progressive results and new ideas.

Past editions of the INTEROP Plugfest were held in Toronto, Canada (IECON 2021); Shanghai, China (ICIT 2022; Kyoto, Japan (ISIE 2021); Singapore (IECON 2020); Lisbon, Portugal (IECON 2019); and in Washington, DC, USA (IECON 2018).

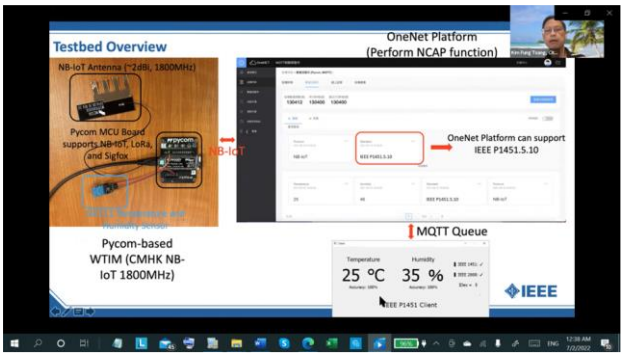


Interoperability demonstration of IEEE P1451.0 platform, INTEROP Plugfest @ ISIE 2021, Kyoto (Courtesy by Russell Trafford)(virtual)

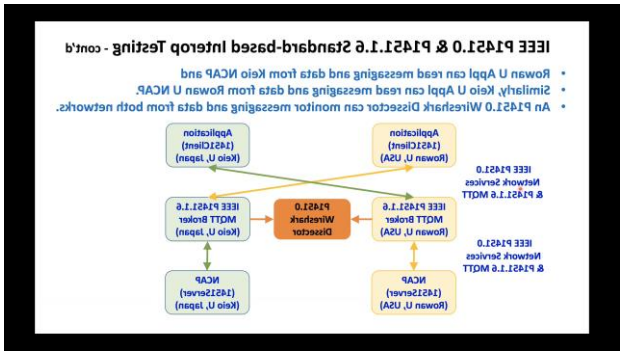
OBJECTIVES

The Objectives of the INTEROP Plugfest are three-fold.

First, to provide the IES Standards community with onsite verification and validation platforms for the standards so the community can test their development of their applications to these benchmarks, ensuring compliance and interoperability to their systems in IES fields of interest. The goal of these platforms is to support users with “turn-key approaches” to their applications, by providing relatively effortless initial start-up processes, allowing easy installation and configuration.



IEEE P1451.5.10 NB-IoT and OneNet Platform Design demonstration at INTEROP Plugfest @ IECON 2021 Toronto (Courtesy Dr. Kim Fung Tsang, City University of Hong Kong)

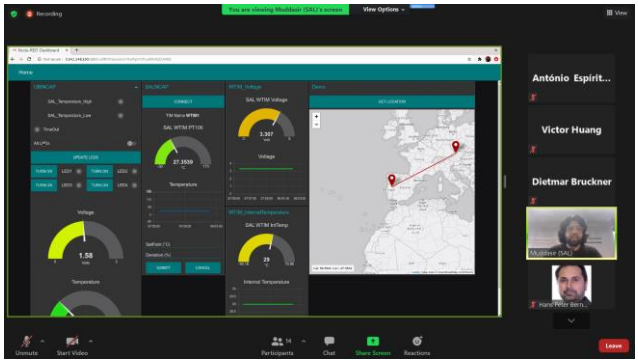


Demonstration IEEE 1451.0 & IEEE 1451.1.6 interoperability @INTEROP Plugfest, IECON 2021 Toronto (Courtesy by Russell Trafford)

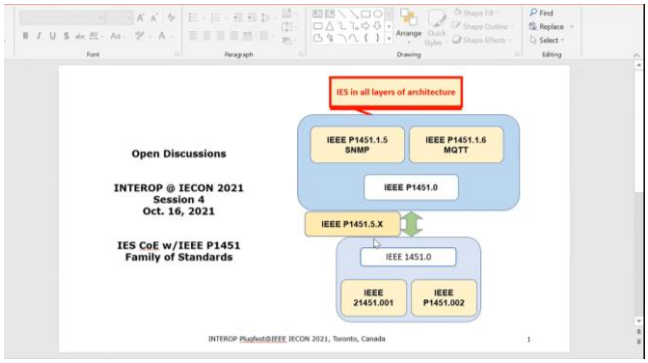
Second, provide a forum for demonstrations and prototypes for interoperability and standards. In addition, a forum for onsite IES standards working groups sessions for active standards discussions and development.

Third, to encourage industry partners to participate in IEEE Standards by providing verification and validation platforms for standards compliance and interoperability in the industry context.

Lastly, and most importantly, the long term goal is to provide stable or permanent validation and compliance Centers of Expertise (COE) for industry and academia use, distributed globally under IES Standards support.



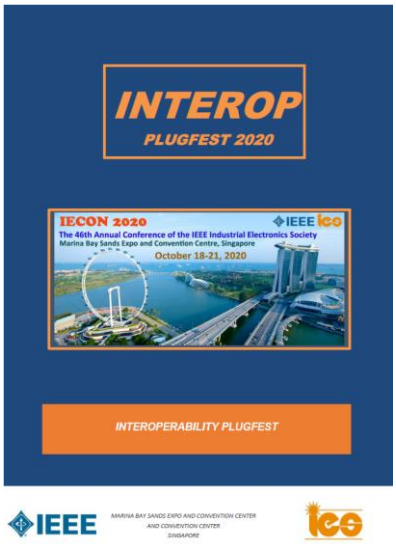
Demonstration showing interoperability between two international locations, INTEROP Plugfest @ ISIE 2021 INTEROP (Courtesy by Hans-Peter Bernhard, Silicon Austria Labs)



Open Discussion on Interoperability @ INTEROP Plugfest Session 4: IES CoE, IECON 2021 Toronto (courtesy by Dr. Victor Huang)

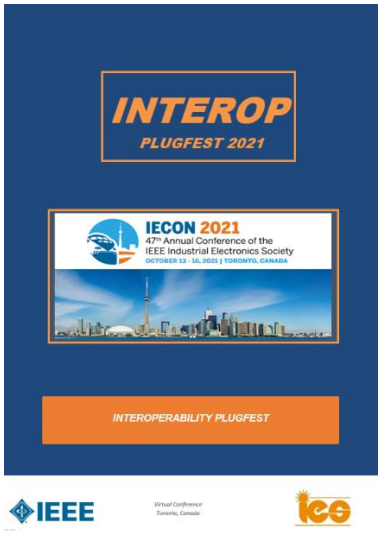
Some actual examples indicating the progress made towards the objectives of interoperability from past INTEROP Plugfests are shown in the previous figures.

PREVIOUS EDITIONS



Brochure of the 3rd INTEROP at IECON 2020 – Singapore

Brochure of the 4rd INTEROP at ISIE 2021 – Kyoto



Brochure of the 5th INTEROP at IECON 2021 – Toronto

TESTIMONIALS FROM PREVIOUS EDITIONS

IECON 2020 *was co-organized by IEEE Industrial Electronics Society, IEEE Industrial Electronics Chapter of Singapore, and the School of Electrical & Electronic Engineering, Nanyang Technological University. Due to COVID-19, the conference was held fully on-line during 18-21 October 2020. The opening ceremony, keynote speeches and* ***INTEROP Plugfest*** *were broadcast live by IEEE.tv. All the remaining sessions were conducted through Zoom, involving real time interactions among speakers and audiences.*

Since INTEROP Plugfest was an important event in IECON 2020, I was invited by Dr Victor Huang, an organizer of INTEROP Plugfest, to join their organizing committee's virtual meetings. Having participated in several INTEROP Plugfest organizing committee meetings, I was deeply impressed by the efficiency that tasks were completed by the committee in time, the enthusiasm and collegiality of the committee members, and most of all the excellent planning and successful execution carried out by the organizers.

All the sessions of IECON 2020, including keynote address sessions, forum/panel sessions of technical activities, tutorials, parallel technical sessions and INTEROP Plugfest sessions attracted active participations of audiences and produced fruitful discussions. The only regret was the lack of physical networking and valuable interaction opportunities during events such as the welcome reception and banquet. In the upcoming IECON 2023, which will be a physical conference held in Singapore, we will provide a wonderful and holistic experience to compensate for this. We look forward to working with INTEROP Plugfest organizing committee in IECON 2023 and meeting the committee members and participants in-person in Singapore.

Professor Changyun Wen
General Chair
IECON 2020 & IECON 2023

IECON 2021 was held from 13-16 October 2021. From having 2938 participants, 13 technical sessions, 77 special sessions, 6 key note speakers and 14 tutorals, the conference also included the **Interop Plugfest.** The **Interop Plugfest** held 4 sessions over 4 days: Automation, IEEE 1451 Wireless Interface, IEEE 1451 Center of Expertise and for the first time, a session on Transportation Electrification and Autonomous Vehicles (TEAM). Both academic and industry partners provided the opportunity for participants to know more about the development of standards in the IES and IEEE community, making the event an unforgettable experience.

Sheldon Williamson Makoto Iwasaki and Kamal Al-Haddad (General Chairs)
Anindita Golder (Conference Secretary)
IECON 2021

INTEROP Demo Summaries

IEEE P21451-1-6 Time Synchronization

IEEE P2992 - Data Expression, Exchange, and Processing in Smart Agriculture

Using Provisioning in IEEE P1451.99 to Assert Ownership of Information

A New Architectural Approach for P1451.99 Binding to P1451.0: a First Proposal for P1451.99.0

Semantic Interoperability in Transducer Management based on IEEE 1451

Demonstration of IEEE P1451.5.X Smart Interfaces for Low Power Wide Area Networks

IEEE P2668 Demonstration for INTEROP 2022

IEEE P1451.1.6

Scope of the proposed standard: This standard defines a method for transporting IEEE 1451 messages over a network using Message Queue Telemetry Transport (MQTT) to establish a lightweight, simplified protocol structure to handle IEEE 1451 communications. The standard uses the common network services defined in IEEE 21451-1.

Purpose: The purpose of this standard is to provide a low-overhead, lightweight method to facilitate IEEE 1451 Communications in systems with low bandwidth, power, or memory allocations.

Need for the Project: MQTT, an application layer protocol, has been widely adapted in the Internet of Things (IoT) paradigm and utilized in large-scale platforms, such as Amazon Web Services, Microsoft Azure, and IBM Watson and, as such, have been adopted by developers in this field. This standard will provide a way for those developers to utilize the IEEE 1451 network architecture and common network services.

What is defined in P1451.1.6?

- Topics naming rules to exchange IEEE1451 messages
- Message data formats to use with MQTT.
- Design of states and processes for maintaining concerning protocols
- IEEE1451 network service messages over MQTT
- Simple and general style of MQTT message to use 1451 devices
- Time synchronization

Message data formats in .1.6

- **D0-OP (Dot Zero Operation)**

IEEE P1451.0-based (Dot Zero-based) Operation (D0-OP) uses the original 1451.0 binary network service messages. It is expected that D0-Message uses new 1451.0 standard messages without any modification. The suffix of the topic name shall start with '_1451.1.6/D0/' given as SPFX and type of message (TOM). The location part of the topic name (LOC) follows the string to be a completed topic name.

- **C-OP (CSV Operation)**

C-OP uses Comma Separated Values (CVS) format, and it can be used as an option. TOM is changed to 'D0C'. The typical example of D0C message topic is '_1451.1.6/D0C/B1/F2/R3'.

C-OP message is perfectly compatible with 1451.0 messages. It simply solves and extends the field size limitation in D0-OP for acquiring usabilities

- **D-OP (Direct Operation)**

D-OP uses a direct format for enabling a more simple and suitable description recommended in MQTT OASIS standard. D-OP is an option. Significant messages are only defined as D-OP, and it strictly observes OASIS MQTT guidelines and general MQTT use cases.

Differences in message types

When using 1451.0 messages over MQTT without any modification, there are some limitations for the use. For exampole, NCAP announcement message is given as follows.

- **D0-OP (binary)**

```
IDL: Args:: UInt16 netSvc0101 {
   in Args::NetSvcType   netSvcType = 1,
   in Args::NetSvcId     netSvcId = 1,
   in Args::MsgType      msgType = 3,
   in Args::UInt16       msgLength (2 bytes),
   in Args::UUID         ncapId,
   in Args::_String      ncapName (length = 16),
   in Args::AddressType  addressType (1:IPv4,
2:IPv6),
   in Args::UInt8Array   ncapAddress (length 4/16
bytes)
};
```

- **C-OP (text)**

1,1,3,ncapId,ncapName,addressType,ncapAddress

Communication Style

NQTTv5 and MQTTv3 extensive rule enable Request-Response style communication adding to MQTT original Publish-Subscribe style communication. 1451.0 is originally developed

Standard for a Smart Transducer Interface for Sensors, Actuators, and Devices - Message Queue Telemetry Transport (MQTT) for Networked Device Communication

West Lab Computing and Networking

on the Request-Response style communication and supposes session (after establishing the session, send and receive functions implicitly identify the communication opposite)

- **Request-Response communication**

This style is generally used in the IP protocols, and is extended for use with MQTT.

Request: NCAP server subscribes to this topic. SPFX, TOM, and concerning descriptors are not included.

Data Request Topic: _1451.1.6/D/LOC of server/DATA/[TIM UUID or TIM NAME]

Data Request Message: The unique topic name to publish the sensor data, shortly [LOC of client]

Response:

Data Response Topic: [LOC of client]

Recommended Data Response Topic: _1451.1.6/D/[LOC of client]/RES/[TIM UUID]

Data Response Message: Sensor Data

NCAP client subscribes to this topic.

- **Publish-Subscribe communication**

This style is the general communication style for MQTT. NCAP server publishes a message to the topic.

Dedicated topic: _1451.1.6/D/LOC/[TIM UUID or TIM NAME]

Compatibility with 1451.0

- **String type format**

String format given in 1451.1.6 is variable length and should use the EOF code to put it at the end of the string in its data expression, which is the same with C language style string rules (to end with NULL character). Originally in 1451.0, _String length of sensor data is limited to 16 characters. The original length of 16 bytes is too short for MQTT topic name. Therefore, SPFX(=_1451.1.6/) and TOM(D0/) are not included in the string.

- **TEDS expression in text fomrat**

Originally, the detail of TEXT TEDS and other text-based format are not given. It is given in P1451.0D2.9. When using C or D operation, the use of TEXT TEDS is recommended.

- **Endian**

Data endian and Network byte order is not defined in 14.51.0. TCP/IP uses big-endian, which sends data from MSB byte order; however, fields order is also not described.

- **Message broadcast**

Discovery process requires IP broadcast/multicast and is rejected in some cases. Therefore, NCAP announcement causes failure in a global network. The discovery process is recommended only for the local (class x) network and cannot be used with cloud or other domains. Collaboration with network searching protocols, such as DNS/DDNS and IEEE 1888, is a considerable solution. MQTT can solve this problem by giving default topics for searching NCAP or distributing NCAP addresses.

- **Session ID is not given**

When multiple accesses have come, it may cause mistakes in message handlings order or a mixture of different streams. 'TimeInstance timestamp' is the only way to distinguish messages. (maybe Ok, but it is messy because it is based on destination numbering, not source numbering.)

- **Client ID is not given**

When the communication sessions are separated and multiply established, it is difficult to establish the return path because there is no way to distinguish the multipe communication lines. IP address and port ID have no meaning in MQTT.

1451.1.6 uses NCAP name for the Client ID. NCAP UUID is a 16byte code and is binary DNS name should be used. Especially, MQTT topic name is consists of strings, such as URI, real addresses, etc. It is inconvenient for the general use. For 1451.1.6, it uses NCAP name to locate the NCAP in the Internet (such as DNS).

Thus, P1451.1.6 solves various problems associated with sending 1451.0 messages using MQTT in its most general form, and provides a simple means to resolve the obstacles that may arise when IoT devices use 1451.

IEEE P2992 - Data Expression, Exchange, and Processing in Smart Agriculture

Future Information Network for Smart Agriculture

Beyond5G and 6G technologies are expected to accelerate the throughput, reduce latency, and improve the interoperability of data services. These technologies will bring game changes.

Low-latency communication improves control precision, and it can improve the performance of agricultural machines and robots. In particular, automated driving and automatic operation of agricultural machines are beneficiaries of these technologies.

Tightly-coupled data interoperability in smart agriculture improves measurement, control, and estimation accuracy. It can improve total service quality. Robust integration of various devices, information, and systems achieve highly value-added services of smart agriculture.

Problems to be solved

These technologies contribute to increasing the benefit but also increase the system cost because these technologies cover the increase in system cost by widening the range of services. Agriculture data can be used for solving a specific problem as well as for solving it broadly.

Additionally, data protection and security of farm management information are indispensable because farm management and farmer data include private information and contain know-how that should be kept secret. It has been fundamentally difficult to Keep important data secret and provide services using that data by using new technologies, such as data anonymization, data encapsulation, and federated learning.

Moreover, general farmers are not experts in handling information and communication. Therefore, it needs a guideline as a standard for Data Expression, Exchange, and Processing in Smart Agriculture

Multiple Service Locations of IoT, Edge, and Cloud

Edge computing, a new concept of computational resources, allows a service-oriented environment. This new edge computing environment enables low-latency communication and service provisioning. However, the essential effect of the use of edge is not limited to low-latency communication. Edge nearby to the farm is safer than the servers in a cloud environment far away. Moreover, new technologies, such as federated learning and message filtering technologies, can provide data-shared services such as AI farming, CO2 trading, system control, and system management without passing on private data.

When focusing on the private data processing in the farm area,

Data Anonymization in edge computing areas is also a crucial function in the future. Data anonymization is achieved by the dedicated data processing of aggregation, generalization, and adding noise to data to make it uniquely unidentifiable. With the anonymization processes, digital watermark using anonymization diversity ensures data users are held accountable in case of

Farm Workers Safety and health management	Farm area Energy control	- Production Management - Regional Power Demand and Supply Management	- Price Management - Import/export management
- To observe crop management - Bureau temperature environment management	House / Field Management and operation	- Cultivation, Growth and Harvest - Pesticide Calendar	- Logistics - Management

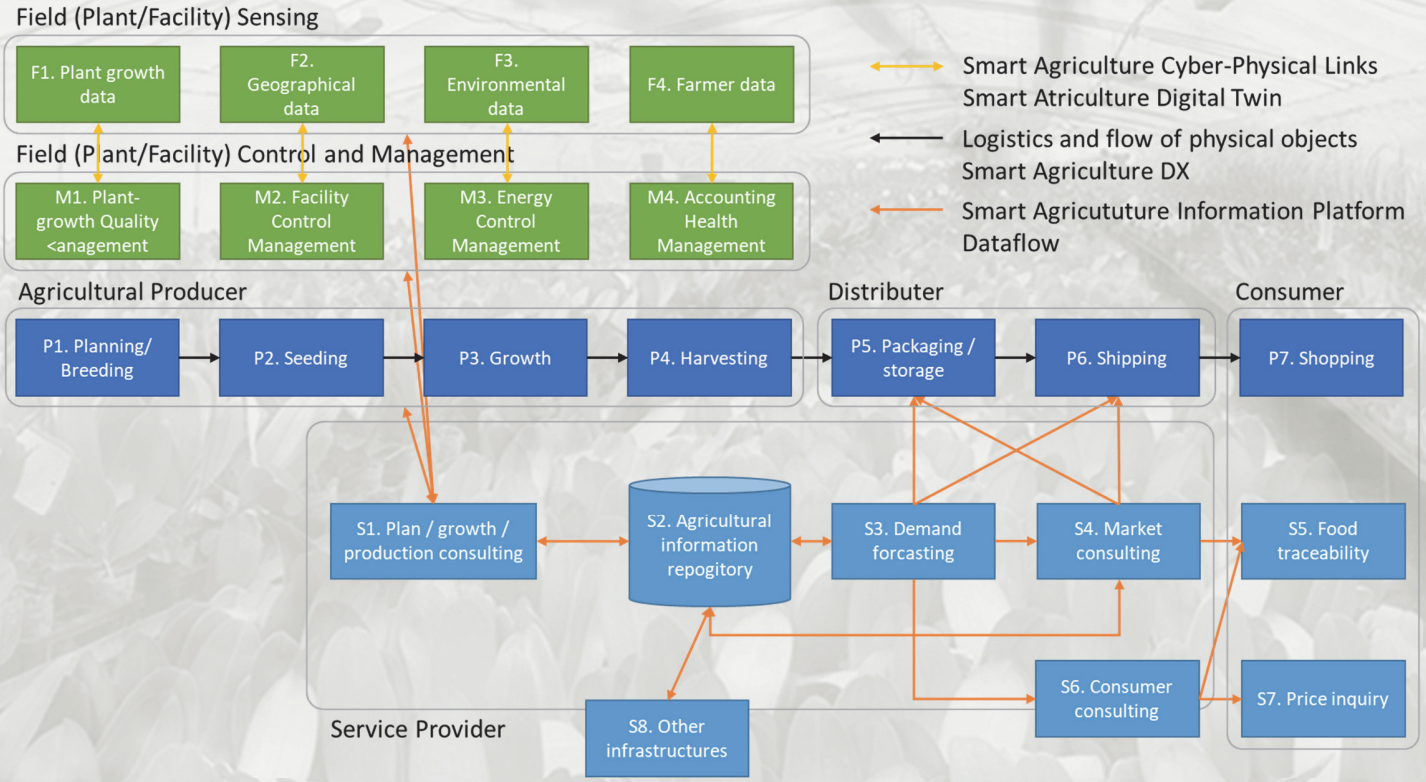
data leakage. Now it has become a big topic to build this kind of data encapsulation technology in certain areas. For example, federated learning provides AI services only by using AI models (neural network parameters learn by using data), not data. Secure computing and secret sharing technology can calculate encrypted data without decrypting

Data-oriented Smart Agriculture

By using the above-described technologies, robust integration of various devices, information, and systems in smart agriculture will achieve highly value-added services

To face this epoch-making era, IEEE P2992 gives the frameworks as given in the following figure.

Moreover, IEEE P2992 will provide the fundamentals for smart agriculture to connect with other smart infrastructures to provide inter-infrastructure smart services.



IEEE P2992

Working Group Name: Data Expression, Exchange, and Processing in Smart Agriculture
Working Group Chair: Hiroaki Nishi , Vice Chair: Rick Zedde
Society and Committee: IEEE Industrial Electronics Society (IES) / IES Standards Committee

Scope of proposed standard: This standard defines recommended practices for designing smart agricul-ture data focusing on the data format, data tags, their naming rules, and data transfers to show the unified practices of data expression, exchange, and processing. This is indispensable for smart agriculture sys-tems, such as data acquisition, data management, data service provi-sioning, and data processing for data security, as well as privacy from the perspective of agricultural machinery control, green-house manage-ment, and farming management. This recommended practice provides the co-existence and interoperabil-ity us-ing common data structure and transfer between heterogeneous systems; namely, various systems of different manufacturers work together to achieve the farmers' requirement efficiently and effectively as for a smart agriculture system.

Need for the Project: Smart agriculture became popular and is indispensable for the current energy and cost-efficient farming industry. There are many kinds of farming industries; however, they use their proprietary systems and are difficult to use togeth-er, especially for cross-data management. This standard provides recommended practices to design the common data infrastruc-ture for smart agriculture to provide the way of co-existence of multiple agricultural data system domains.

Using Provisioning in IEEE P1451.99 to Assert Ownership of Information

Peter Waher
R&D
Trust Anchor Group Chile SpA
Concon, Chile
peter.waher@ieee.org

***Abstract*—In open interoperable networks on the Internet, it has often been assumed ownership of information is lost, as traditional infrastructure has no mechanism to control access once it has been released to in open networks. The available proposal in P1451.99 IoT Harmonization changes this. It provides a mechanism to define unique ownership of things in open and interoperable internetworks, and a method to authorize access to information and operations, in a very detailed fine granular level. This proposal therefore permits open, interoperable, and secure internetworks to be created, using zero-configuration, from the infrastructure or operator perspective. This provisioning capability of P1451.99 will be presented to participants, who can use a freely downloadable App (on Android or iOS) to experiment.**

Introduction

Information ownership is not protected by law, except in very rare exceptions, such as information that can be considered Intellectual Property, or patentable. This is especially the case when it comes to the Internet of Things. Each Thing, be it a sensor, activator, or a more complex construct, typically produces a lot of information, often valuable information. These Things also typically cost money to buy, install and operate. But unless there's a method to protect the ownership of the information these Things generate, or the services they provide, there is no incentive for investors in Things to publish them in open networks, for others to use. This is particularly the case in Industry. Why would you allow a competitor to use your devices, if it only generates stress and load on your system, while the competitor gets the information for free, possibly creating exploitable vulnerabilities in the process? This fact has limited the development of IoT, compared to original forecasts. Instead of investing in interoperable networks, companies prefer closed networks and proprietary technologies. Any standard aiming at creating Interoperability across domains, must take this into account: It must include a mechanism whereby owners of devices can authorize access to them, at a very fine granular level, in an automatable manner. This method must also not place unproportional load on the operator of the infrastructure, meaning it cannot require manual operation or intervention by anyone, except possibly the owners themselves, and the parties requesting access to the corresponding information or operations. This is often referred to as *zero-configuration networking*.

Standard Overview

The interfaces of the current proposal of IEEE P1451.99 IoT Harmonization [1] provides a series of peer-to-peer and edge services, and features that help in the creation of open, interoperable, and secure networks for things. It is based on the XMPP protocol, which is standardized by the Internet Engineering Task Force [2]. XMPP was originally designed as a protocol for Instant Messaging, with the goal of creating interoperability and to protect privacy and security of users communicating privately with each other over the Internet. Its flexibility allows it also to become a common ground of harmonization of protocols of varying types and architectures. Its security mechanisms provide a good starting-point on which an IoT Harmonization standard can be built. The following list shows features and services added by the current IEEE P1451.99 proposal on-top of XMPP. This paper, and the corresponding demo during the Interop Plug fest, will focus on the emphasized items.

- Identity
- Communication Patterns
- Sensor Data
- Control Operations
- Localization (M2M, M2H)
- Tokens for distributed transactions
- **Decision Support (for devices)**
- **Provisioning (for owners)**
- Peer-to-Peer communication
- End-to-end encryption
- Concentrator/Bridge ("Thing of things")
- Discovery
- **Ownership**
- Clock/Event Synchronization
- Secure Account Creation
- Remote Updates
- Legal Identities
- Smart Contracts
- Automated provisioning

Provisioning

IEEE P1451.99 contains harmonized interfaces for interacting with sensors, actuators, and things in general. Each provisioned device in the network has a unique owner. This owner is responsible for providing the decision support system with information on how third parties can interact with their devices. When a provisioned thing receives a request, it does not know how to handle, it asks the underlying decision support edge service what it is supposed

to do. If the service knows, it replies. Replies can be either “Yes”, “No”, or “Partial”, in which the thing restricts the original request to include only what the owner authorizes.

If the decision support edge service does not know what to do, it always tells the device No. At the same time, a message is pushed to the owner, which may be a slow human. The owner, in turn, responds in its time. Through these responses, the decision support service learns, and the next time the thing asks for help, it can respond in a better way, and always in accordance with the specifications of the corresponding owner (Fig. 1).

Material and Equipment

The demonstration will include the following components:

- Remotely connected devices, accessible via Internet, and visible via Web Camera. Links will be provided during presentation.
- Internet-devices bridged to P1451.99, accessible via Internet.
- Simulated devices, accessible via Internet, generated by open-source simulator ComSim [3] (Fig. 2). Links will be provided during presentation.
- Free open-source app [4] (compliant with latest IEEE P1451.99 proposal), available via Google Play Store [5] for Android and Apple App Store [6] for iOS. (Fig. 3)

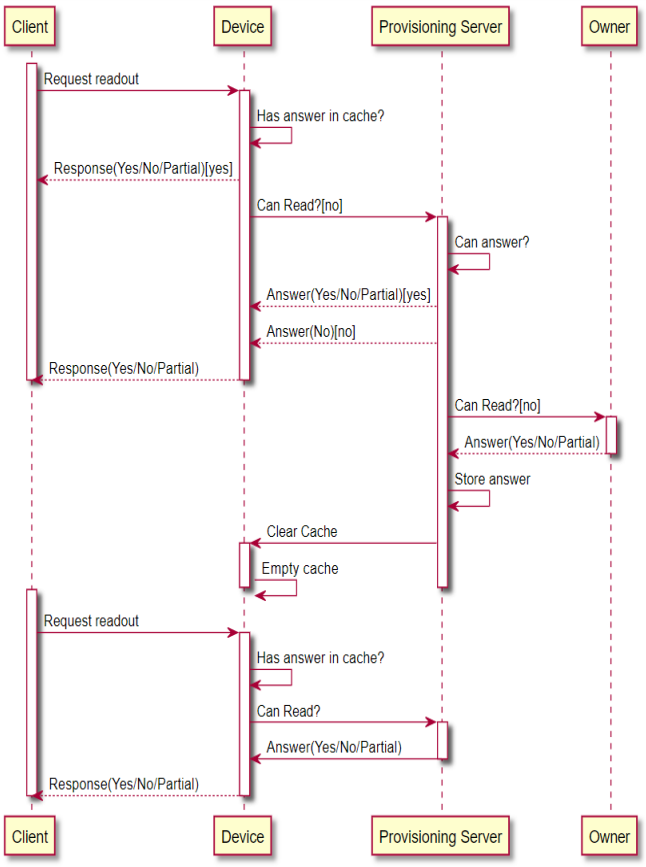


Fig. 3. *IEEE P1451.99 Provisionins Service providing real-time decision support to a device, based on Owners wishes.*

Fig. 1. *TAG digital ID App - main page*

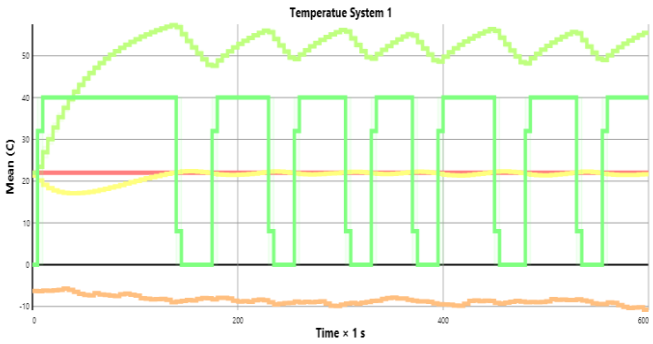


Fig. 2. *ComSim – automatically generated graph of simulated device*

References

[1] IEEE 1451.99 WG Open Source Repository for XMPP IoT Interfaces: https://gitlab.com/IEEE-SA/XMPPI/IoT, retrieved Sept 2022.

[2] P. Saint-Andre, “Extensible Messaging and Presence Protocol (XMPP): Core”, RFC 6120, “Instant Messaging and Presence”, RFC 6121, “Address Format”, RFC 6122, Internet Engineering Task Force (IETF).

[3] Open Source TAG ComSim repository on GitHub, for simulating human behavior at scale, https://github.com/Trust-Anchor-Group/ComSim, Trust Anchor Group AB, retrieved May 2022.

[4] Open Source TAG Digital ID App repository on GitHub, for Android and iOS, https://github.com/Trust-Anchor-Group/IdApp, Trust Anchor Group AB, retrieved May 2022.

[5] Free TAG Digital ID for Android, published in Google Play Store, https://play.google.com/store/apps/details?id=com.tag.IdApp, retrieved May 2022.

[6] Free TAG Digital ID for iOS, published in Apple App Store, https://apps.apple.com/se/app/trust-anchor-id/id1580610247?l=en, retrieved September 2022.

A New Architectural Approach for P1451.99 Binding to P1451.0: a First Proposal for P1451.99.0

Riccardo Brama
IEEE P1451.99 Chair
Cortus S.r.l.
Lecce (IT)
0000-0003-4270-1828

Peter Waher
R&D
Trust Anchor Group Chile SpA
Concon, Chile
peter.waher@ieee.org

***Abstract*—This demo demonstrates both a new proposal for aligning P1451.99 with the newly introduced 1451 standard family architecture and casts the basis for a JSON based generalized binding interface, P1451.99.0, to make arbitrary IoT verticals fully compliant with IEEE P1451.0 ecosystem.**

Introduction

Never as in these days the harmonization of different verticals of Internet of Things (IoT) and IIoT (Industrial Internet of Things) is becoming of critical importance. Gathering information from different devices using a uniform approach, while easing the adoption of a common interface to systems yet deployed on the field, allows to minimize the need for systems duplication thus minimizing both costs and the impact of human activities on the environment. The first proposal for P1451.99 has been designed to become a distributed, privacy and security enforcing IoT common ground whose network architecture is reliable and fault tolerant.

After the revision of P1451.0, introducing an in-depth reshaping of the overall 1451 Standards Family, it became evident how the P1451.99 architecture needs to be backed by a set of ancillary interfaces allowing the various P1451.1.X communication stack flavors to fully take advantage of P1451.99 harmonized things.

Standard Overview

At the beginning of its development path, the IEEE P1451.99 IoT Harmonization was designed to provide a series of services and features to ease the creation of an open, interoperable, and secure network ecosystem for things. The basis for this harmonization layer has been identified in the XMPP protocol, originally standardized by the Internet Engineering Task Force [1] for Instant Messaging, and on the IEEE P1451.1.4 communication stack as the gateway for reaching P1451.99 harmonized network [2]. The P1451.99 has been kept as agnostic as possible with respect to underlying technologies to be harmonized. This to make it neutral and cross-domain. It is interesting to note that the first P1451.99 proposal is purposely agnostic of both the 1451.0 messaging and insights. This because the P1451.1.4 had to provide mechanisms and resources allowing to bridge the 1451.0 ecosystem with the P1451.99. The new 1451 standards family asset proposed by the P1451.0, on the other hand, suggest P1451.1.4 to be an independent XMPP implementation, urging the need to reshape the P1451.99 aligning it with this new vision.

To bind the P1451.0 ecosystem with the P1451.99 it has been proposed an architecture in which the P1451.99 ecosystem is the center around which both 1451 enabled devices and non-1451 enabled networks can join. Binding is realized by means of IP enabled gateways that from one side can interface with any of the P1451.1.X standards and, on the other, implement the entire P1451.99 protocol stack to reach the harmonized IoT level. These gateways will provide the following features:

- Realize binding between JIDs identified Concentrators/Nodes and IEEE P1451.0 UUIDs;
- Real time generation of TEDS for non-1451 enabled IoT verticals, possibly with proxying capability;
- Translation of non-1451 messages towards P1451.99;
- Adaptation of P1451.99 messages towards the corresponding P1451.1.X layer.

Implementing this set of features for each P1451.1.X member is a straightforward work due to the perfect knowledge of the P1451.1.X insights. At the same time, it is easy to integrate other well-known technologies, such as the newborn Matter [3], in an harmonized P1451.99 ecosystem. On the other hand, it is more challenging to address arbitrary non-1451 verticals. This can be done only abstracting completely implementation details focusing only on data and its informative content.

A two layers abstraction proposal for the P1451.99.0 general binding is shown in Fig. 1.

The first layer, the Specific Gateway Interface (SGI) provides a set of primitives defining a common interface that developers must implement to interface with an arbitrary networking technology. This layer abstracts all communication details while keeping information about addressing needs, devices and users' identity (where applicable), and devices capabilities. In other terms it provides a uniform interface for arbitrary non-1451 IoT verticals.

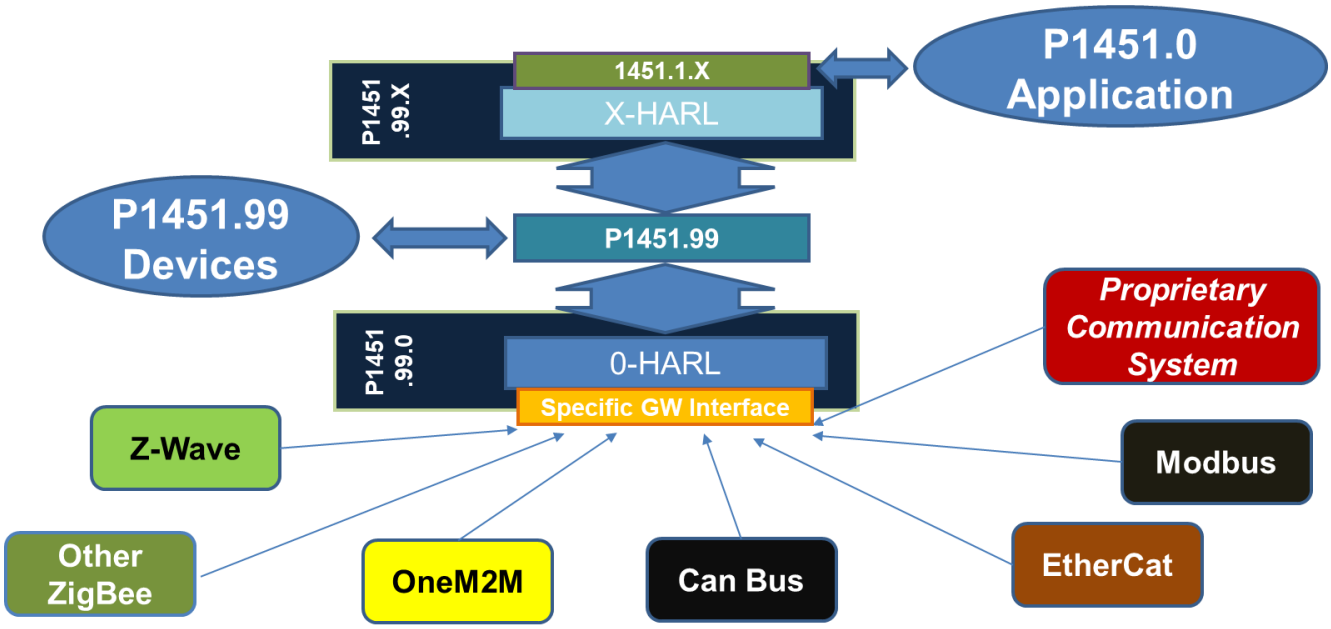


Figure 1 The proposed P1451.99 Centric Binding Approach

The second layer, the Harmonization Layer (HARL), is the one in charge of both message translation and of TEDS generation and proxying service.

To realize such a goal the HARL needs to be aware of a set of information that shall be provided from the SGI abstracted network. In the 0-HARL, i.e. the HARL of the P1451.99.0 binding, this is realized by means of a JSON based information representation [4]. Each device of the SGI abstracted interface is described with a proper JSON object whose methods are well known and documented. It will be beyond the scope of the P1451.99.0 taking care of security and privacy details within the premises of the SGI abstracted network.

Collecting information on SGI network device capabilities the 0-HARL can compile TEDS in an appropriate P1451.0 format. These TEDS are then used to describe in a fully compliant 1451.0 way the non-1451 devices.

In the same way JSON objects, together with primitives, can be used to provide a representation of actions and their informative content needed to interface the P1451.99 harmonized network towards the SGI network.

Material and Equipment

The demonstration can be carried out by means of a personal computer as a way to mimic both the non-1451 side and the P1451.99.0 gateway.

Demo Structure

The demonstration will limit to show how it is possible to compile a TEDS from an abstracted JSON description of an arbitrary object in a non-1451 SGI abstracted network as shown in Fig. 2. The non-1451 side of the communication symbolizes an arbitrary gateway implementing, at least the SGI abstraction layer. The P1451.99.0 binding provides initialization, JID generation, TEDS completion and caching allowing to produce a full 1451.0 compliant TEDS that can be retrieved from another P1451.99.X binding through the P1451.99 network.

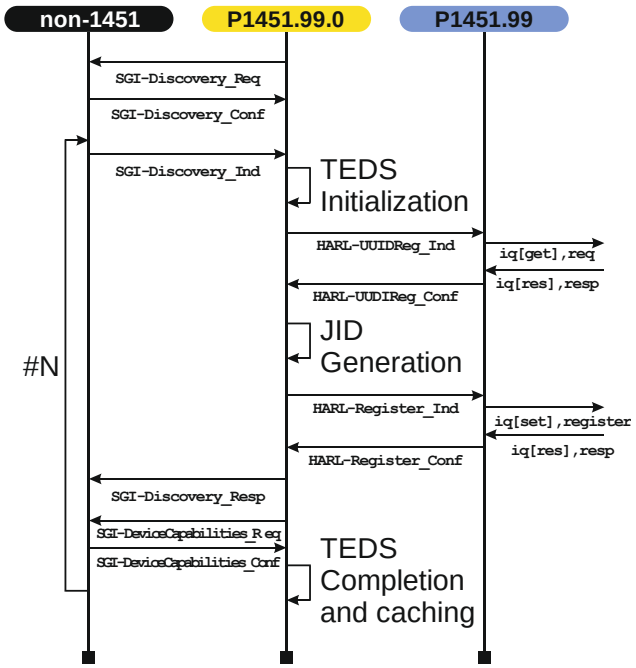


Figure 2 TEDS Caching Service

References

[1] P. Saint-Andre, "Extensible Messaging and Presence Protocol (XMPP): Core", RFC 6120, "Instant Messaging and Presence", RFC 6121, "Address Format", RFC 6122, Internet Engineering Task Force (IETF).

[2] IEEE 1451.99 WG Open Source Repository for XMPP IoT Interfaces: https://gitlab.com/IEEE-SA/XMPPI/IoT, retrieved Sept 2022.

[3] Connectivity Standards Alliance, "Matter", https://csa-iot.org/

[4] T. Bray, "The JavaScript Object Notation (JSON) Data Interchange Format", RFC 8259, Internet Engineering Task Force (IETF)

Semantic Interoperability in Transducer Management based on IEEE 1451

Helbert da Rocha
Dept. of Electromechanical Engineering
University of Beira Interior
IT – Institute of Telecommunications
Covilha, Portugal
helbert.rocha@ubi.pt

João Luís Dâmaso Pereira
Dept. of Electromechanical Engineering
University of Beira Interior
IT – Institute of Telecommunications
Covilha, Portugal
joao.luis.pereira@ubi.pt

Antonio Espirito Santo
Dept. of Electromechanical Engineering
University of Beira Interior
IT – Institute of Telecommunications
Covilha, Portugal
aes@ubi.pt

Abstract-The IEEE 1451 standard has the potential to be a good choice for the digitalisation of the shop floor or factory floor. It was designed for the transducer management on it is used in the Industrial Internet of Things, inside the manufacturing process known as Industry 4.0 composed by the Cyber-Physical Systems and to its digital representation the Digital Twin. The Instrumentation and Measurement laboratory has been working on open access online platforms designs and validates IEEE 1451 compliant transducers. Users can create, edit, and manage Transducer Electronic Data Sheets and export the code to a Transducer Interface Module. Also, a new semantic communication layer is proposed inside the Network Capable Application Processor to supply the need for semantic communication based on an IEEE 1451 vocabulary inside Industry 4.0.

Introduction

The interoperability allows communication between devices of different vendors inside an industrial context. Industry 4.0 requires a semantic level of communication between the devices connected on the shop floor. The IEEE 1451 standards at the current level of standardisation reach the syntactical level of interoperability. To reach a semantic level, it needs to use a framework, such as OPC UA or oneM2M.

To permit the IEEE 1451 standards at the communication level to reach a semantic level. A new heavyweight ontology and vocabulary were developed. It is open to access and open to everyone to use on their own lightweight ontology employing the IEEE 1451 for transducer communication, as shown in Fig 1.

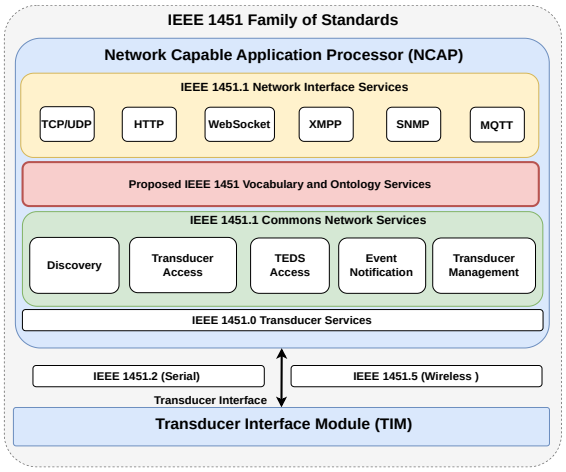


Fig. 1 Proposed Semantic Layer.

Semantic Layer development

The new proposed layer was developed using the Semantic web stack, widely used for the current Internet communication, as shown in Fig.2. It is composed of linked data that uses the Unified Resource Identifier (URI) to link the data to the place where the information is stored. The information is serialised using XML or JSON format. Employing JSON-Linked Data (JSON-LD) is possible to create a context for the communication. This context is used to represent each component during the communication process.

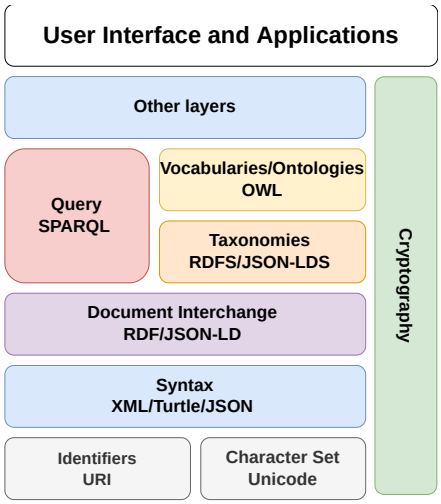


Fig. 2. Semantic web Stack.

Semantic Layer Encode and Decode

The JSON-LD was utilised for encoding the data during the communication. It allows for creating an IEEE 1451 context based on the vocabulary proposed by the IEEE 1451 standards.

The NCAP translates the octets commends from the TIM and creates the structure to communicate using JSON serialisation. The JSON-LD allows adding a context for the communication, present in Fig.3. This context is sent inside the JSON using the MQTT or HTTP protocols, for example. The application that receives the information decodes the communication using the same context, as shown in Fig.4. This allows the application to know the data formats used during the communication when this information is needed. It is easy to read for humans and machines.

```
{
  "@context": "http://iml.ubi.pt/2022/ieee1451/ieee1451.jsonld",
  "NCAP": {
    "NCAPManufactureID": "IML2022",
    "NCAPModelNumber": "0.2",
    "NCAPSerialNumber": "5",
    "NCAPOSVersion": "0.3",
    "TIM":[{
      "timId": "1",
      "MetaTEDS": {
        "TEDSLength": "59",
        "tedsID ": "1",
        "UUID": "040A91B3501A6945F9817ED1",
        "oHoldOff": "1",
        "sHoldOff": "1",
        "testTime": "1",
        "maxChan": "4",
        "cGroup": {
          "grpType": "1",
          "memList": "1"
        }
      },
```


Fig. 3. IEEE 1451 semantic encode.


```
{"http://www.iml.ubi.pt/2022/ieee1451#NCAP": {
"http://www.iml.ubi.pt/2022/ieee1451#NCAPOSVersion": { "@type":
"http://www.iml.ubi.pt/2022/ieee1451#String",
    "@value": "0.3"},
"http://www.iml.ubi.pt/2022/ieee1451#NCAPManufactureID": { "@type":
"http://www.iml.ubi.pt/2022/ieee1451#String",
    "@value": "IML2022" },
"http://www.iml.ubi.pt/2022/ieee1451#NCAPModelNumber": {  "@type":
"http://www.iml.ubi.pt/2022/ieee1451#String",
    "@value": "0.2" },
"http://www.iml.ubi.pt/2022/ieee1451#NCAPSerialNumber": {"@type":
"http://www.iml.ubi.pt/2022/ieee1451#String",
    "@value": "5"},
  "http://www.iml.ubi.pt/2022/ieee1451#TIM": {
 "http://www.iml.ubi.pt/2022/ieee1451#MetaTEDS":
{"http://www.iml.ubi.pt/2022/ieee1451#TEDSLength": {"@type":
"http://www.iml.ubi.pt/2022/ieee1451#UInt32",
      "@value": "59"},
"http://www.iml.ubi.pt/2022/ieee1451#UUID":
"040A91B3501A6945F9817ED1",
 "http://www.iml.ubi.pt/2022/ieee1451#oHoldOff": {
      "@type": "http://www.iml.ubi.pt/2022/ieee1451#Float32",
      "@value": "1"},
```


Fig. 4 IEEE 1451 semantic decode.

DIGITAL TWIN EXAMPLE

A Digital Twin for monitoring and visualisation was developed to show how a new proposed communication layer can be employed. It uses the MSP430F5529 USB Experimenter's Board as TIM connected to a water level sensor and a temperature sensor, and a Raspberry Pi B+ as an NCAP. It simulates a painting part of a shop floor car manufacturing, as shown in Fig.5.

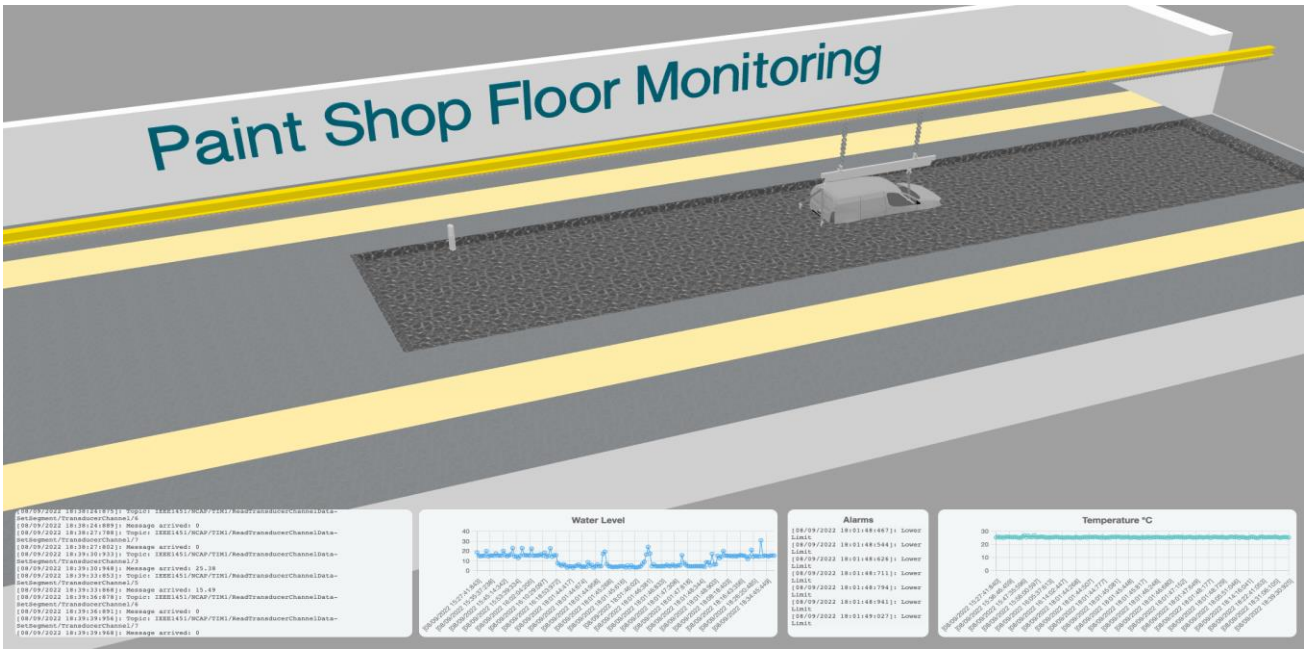


Fig. 5. Digital Twin with IEEE 1451 standards.

Demonstration of IEEE P1451.5.X Smart Interfaces for Low Power Wide Area Networks

Zhifu ZHANG and Kim Fung TSANG*
Department of Electrical Engineering
City University of Hong Kong
Hong Kong SAR
*ee330015@cityu.edu.hk

***Abstract*—The IEEE P1451.5.x standards is developing a universal standardized smart transducer interface which provides "plug-and-play", authentication, time synchronization, interoperability, and security for devices in low power wide area networks (LPWANs, including e.g., Long Range (LoRa), NB-IoT, Sigfox). Each of the major LPWAN technologies (e.g., Long Range (LoRa), NB-IoT, Sigfox) has its respective sub-standard in the IEEE P1451.5.x family. In which, IEEE P1451.5.5 corresponds to LoRa; IEEE P1451.5.6 corresponds to Sigfox; IEEE P1451.5.10 corresponds to NB-IoT. The IEEE P1451.5.x standard defined wireless transducer interface module (WTIM as the device node in the networks), uses transducer electronic data sheet (TEDS describing the WTIM, defined in IEEE P1451.0), and network capable application processer (NCAP as the network server, defined in IEEE P1451.0) to propose a standardized smart interface for LPWANs. The IEEE P1451.5.x aims to mitigate the LPWAN compliance issue and to realize "Plug-and-Play" features.**

I. Introduction

With the trending industrial 4.0 development in building smart city, smart public transportation, smart environmental monitoring system, etc., the internet of things (IoT) as one of the supporting technologies is growling vigorously without standards to solve the compliance and interoperability issues. In IoT, Long Range (LoRa), NB-IoT and Sigfox are the 3 major LPWAN technologies in which kilo-number level devices (transducers) can be deployed. Using ISM free licensed band, LoRa is capable of deploying private secure kilometer-level coverage networks either by personal or organization. It's low power, low cost and high sensitivity led to continuously growing of deployed applications and WTIMs that enlarges the issues of interference and compliance due to non-standardization in the industry. Sigfox, like LoRa, applies the ISN un-licensed band, whereas NB-IoT adapts the cellular mobile network provided by internet services provider (ISP) in the licensed band and took the advantages of the current mobile networks. The users can choose the three based on their usage and requirements.

The IEEE P1451.5.x standard is developed under the IEEE P1451 family which defined the transducer electric data sheet (TEDS), wireless transducer interface module (WTIM), network capable application processor (NCAP) and communication APIs used in the development of IEEE P1451.5.x standard.

The WTIM, defined in P1451.0[1] is the devices (i.e., the end nodes performing the various designated functions such as: sensors collecting information, actuators performing commands transmitted from NCAP applications, etc.) in the LPWAN IoT networks. The TEDS, defined in P1451.0 contains information describing each WTIM. The information includes wireless transmission configurations (e.g., the data format in the payload, transmission interval, payload size, WTIM operation mode, etc.), authentication keys (e.g., device unique identifier, subscriber's identity module (SIM card) (for NB-IoT devices using cellular networks for transmission), NCAP application authentication keys, etc.) for joining IoT networks, sensor configurations (e.g., data type of the collected sensory information, processing steps, etc.) etc. By proper usage of the TEDS, WTIM is able to realize the "plug-and-play" feature without further human configurations. The NCAP, defined by IEEE P1451.0, is also the network server in P1451.5.x standards that manages the joined devices (WTIMs) and transfer data between the WTIMs and the 1451 clients (i.e., NCAP applications). The communication API defined by IEEE P1451.0 is the standardized API for TEDS decoding in WTIM, WTIM configuration, wireless transmissions (using various technologies e.g., LoRa, NB-IoT, Sigfox, Wi-Fi, Bluetooth, etc.) between WTIM and NCAP, and TEDS verification in NCAP.

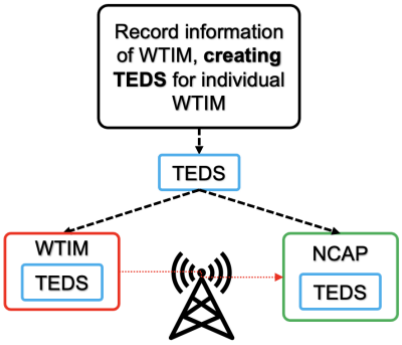


Fig. 1 TEDS working flow

The NCAP receives the transmissions from the WTIM and derives the configurations of the WTIM in the physical layer by calling communication API. In NCAP, the derived configurations are then compared and verified to see if the WTIM is correctly configured.

II. The Design of The Standardized System

A. TEDS configurationa and authentication in the WTIM

Each WTIM has a TEDS that records all the information necessary for the WTIM to join the respective LPWAN and transmits to NCAP. WTIM will configure its physical wireless transmission according to the content inside the TEDS to perform the transmissions in the LPWAN. The configuration will be completed using the communication API defined in IEEE P1451.0[1].

WTIM firstly decodes and extracts content inside the TEDS. The extracted specifications are applied to initially configure the wireless transmission module in WTIM in physical layer (e.g., LoRa region, NB-IoT frequency band, Sigfox transmission intervals, etc.). The extracted specifications (e.g., LoRa Dev_EUI, App_EUI; NB-IoT Access Point Name (APN), EARFCN, etc.) are also used to join the respective LPWAN of each WTIM. Then, the WTIM uses communication API transmits to NCAP.

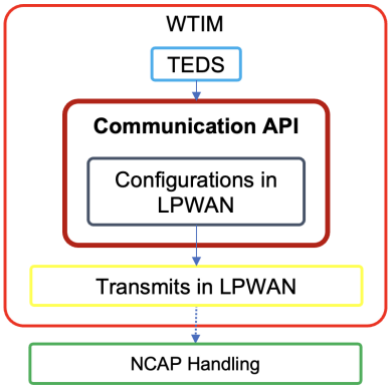


Fig. 2 TEDS distribution to WTIM

B. *TEDS verification in the NCAP*

NCAP receives the transmissions from WTIM and derives the wireless transmissions of the WTIM (e.g., transmission interval, etc.) using communication API. The communication API will the compare the derived configurations with the TEDS distributed to the NCAP when deploying the LPWAN for required applications. If the configurations derived from the transmissions do not equal to the corresponding content in the TEDS, the WTIM is then deemed to be not following the standard.

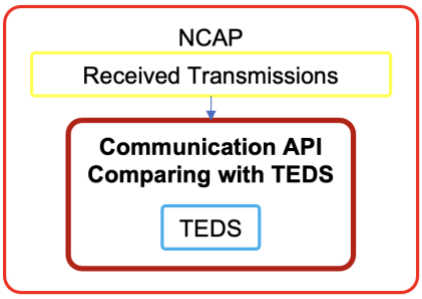


Fig. 3 TEDS verification in NCAP

C. *Communication APIs*

The communication APIs are defined with reference to IEEE P1451.0 standard[1]. The APIs have several functionalities in both WTIM and NCAP and it functions in both the physical layer and the application layer. When the WTIM is authenticated in the LPWAN and joined the network, the communication API is then used for payload transmission. For LoRa WTIM, the API performs its functionalities in physical layer using LoRa radio due to whose technical limitations. For NB-IoT WTIM, the API transmits information using application layer internet protocols (defined in IEEE P1451.1[3] standard) such as message queuing telemetry transport (MQTT), constrained application protocol (CoAP) due to the relative redundant network resources of NB-IoT networks. The IEEE P1451.0 standard defined APIs in both layers in WTIM.

The IEEE P1451.0-standardized communication APIs in NCAP performs WTIM authentication, transmission reception, configuration deriving, and TEDS verification. The results of the TEDS verification with respect to certain individual WTIM can be extracted to NCAP applications for further procedures to be taken (e.g., reject the further transmission from the specific WTIM, issue downlink commands asking WTIM to modify the conflicted settings, etc.).

III. Demonstration

A. *Material and Equipment*

The demonstration is based on the introduction of IEEE P1451 and LPWAN. Material and Equipment required include (1) IEEE P1451.0, .1 and .5.x standard family; (2) LPWAN systems including end node devices for each respective LPWA technologies (LoRa, NB-IoT, Sigfox); gateways and ISP cellular networks for wireless transmissions between WTIMs and NCAP; NCAP servers.

B. *Demonstration Structure*

Based on the standardization work of IEEE P1451, for LPWANs, a MCU based standardized structure is presented. Developers could reference the structure to develop the WTIM products.

In the proposed model, an Arduino-based MCU is proposed to control the LPWAN communication modules and transducers. For instance, the MCU collects the temperature or humidity data from transducer sensory interface and these data are then transmitted to NCAP by LoRa, NB-IoT or Sigfox modules. In the MCU, the TEDSs and communication, control APIs are developed by the developers as embedded software in the storage of MCU. In the NCAP, the communication and control APIs are also developed to verify the transmissions between LPWAN WTIMs and NCAPs. The results of the verification can then be sent to NCAP applications deciding if the NCAP should reject the transmissions sent from the WTIM. With this design, the whole LPWAN system are standardized and the WTIMs can access into the network with “Plug-and-Play” feature.

IV. Useful Links and Additional Resources

- IEEE P1451.5.5 LoRa Main page: https://standards.ieee.org/ieee/1451.5.5/10611/
- IEEE P1451.5.6 Sigfox Main page: https://standards.ieee.org/ieee/1451.5.6/10612/
- IEEE P1451.5.10 NB-IoT Main page: https://standards.ieee.org/ieee/1451.5.10/10613/

V. References

[1] "IEEE Standard for a Smart Transducer Interface for Sensors and Actuators - Common Functions, Communication Protocols, and Transducer Electronic Data Sheet (TEDS) Formats," in IEEE Std 1451.0- 2007 , vol., no., pp.1-335, 21 Sept. 2007

[2] "IEEE Standard for a Smart Transducer Interface for Sensors and Actuator -- Wireless Communication Protocols and Transducer Electronic Data Sheet (TEDS) Formats," in IEEE Std 1451.5-2007 , vol., no., pp.1- 225, 5 Oct. 2007

[3] "IEEE Standard for a Smart Transducer Interface for Sensors and Actuators - Network Capable Application Processor Information Model," in IEEE Std 1451.1-1999 , vol., no., pp.1-480, 18 April 2000

IEEE P2668 Demonstration for INTEROP 2022

Yo-Che LEE and Kim Fung TSANG*
Department of Electrical Engineering
City University of Hong Kong
Hong Kong SAR
*ee330015@cityu.edu.hk

***Abstract*— The vast utilization of Internet of Things (IoT) has engendered challenges in the implementation of large-scale IoT systems. For instance, for the Government-Wide IoT Network (GWIN), a city-wide IoT Network, supporting smart city development, it is challenging to evaluate the performance and the acceptability of the application. In response to such an issue, the IEEE P2668 Standards Working Group has developed the IoT Maturity Index, or IDex, to evaluate IoT objects from the perspective of their performances and applications. Following previous INTEROPs, this article provides an overview of IDex development and introduces the demonstration session to be given in INTEROP 2022.**

I. INTRODUCTION

The concept of Internet of Things (IoT) connects various objects to the internet. It has incubated a generation of smart applications in various fields, including agriculture, healthcare, and smart living, with the aim of making people's life more convenient. Along with the vast growth of applications is the inflating interest in large-scale IoT systems and smart application development. As the concept of the smart city emerged, the scale of an IoT system has grown from a room, a building, to an entire city. For instance, the Government-Wide IoT Network (GWIN) is a city-wide network of sensors scattered throughout Hong Kong, based on the LoRa Wide Area Network (LoRaWAN), supporting various smart applications to improve the quality of public service [1].

However, handling such a large-scale system is not facile. Challenges may be encountered as the complexity of an IoT system rises due to the multiple layers of infrastructure, service, and policies. One of the concerning issues is the quantification of the performance of a large-scale IoT system, as it is needed for grading, ranking, and evaluation. For instance, to conduct a Distributed Denial of Service (DDoS) [2] penetration test on a high-availability large-scale system protected by a firewall, such quantification and evaluation method is needed to reflect the impact of the penetration test on the system and the effectiveness of the firewall module for analysis.

To solve such problems, the IEEE P2668 family of standards defines the IoT maturity index, referred as IDex, to systematically measure the maturity of IoT objects in a standardized manner [3]. From a one to five level, the IDex will cover the whole IoT ecosystem, from infrastructure, service, network, application, to policy. In different layers and their sublayers, with evaluations of various criteria defined in IDex and their weighting, an overall IDex can be calculated to reflect the overall maturity of an IoT system.

In this article, an overview of the IEEE P2668 standards and IDex will be provided. In the demonstration, the flow of IDex evaluation will be presented under the scene of a DDoS penetration test on an IoT system.

II. STANDARD OVERVIEW

The IEEE P2668 measures the maturity of IoT objects, objects in the IoT environment, including equipment, things, or the entire system [3]. Aiming to facilitate the comparison, adoption, development, and selection of IoT products efficiently blending them into a system with better performance, the IDex provides a quantitative indication of the performance of IoT objects from multiple levels.

The IDex classifies an IoT object into five levels, from the range of 1 to 5, where the IDex 5 indicates the highest maturity, while the IDex 1 denotes the lowest maturity of an IoT object. Additionally, the IDex score can be represented by any real number between 0 and 5, which can be converted to discrete one-to-five IDex levels. To cover all the objects in an IoT environment, there are five formats of IDex customized for different infrastructural fields, as shown in Figure 1.

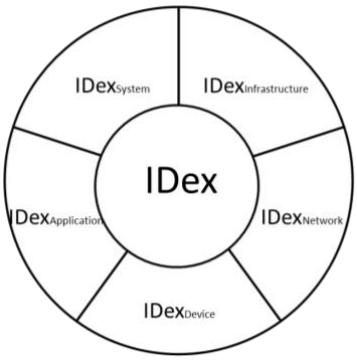


Fig. 1. Formats of IDex for different infrastructural field

The $IDex_{Device}$ evaluates the maturity of an IoT object at the device level, which can refer to a machine, sensor, actuator, controller, microprocessor, transducer, etc. The $IDex_{Network}$ evaluates the maturity of an IoT object at the device level, which includes a communication protocol, network topology, computer network, radio network, middleware, etc. The $IDex_{Application}$ evaluates the maturity of an IoT object at the application level, which can refer to control, scheme, administration, management, analytics, etc. The $IDex_{Infrastructure}$ evaluates the maturity of an IoT object of an integration of multiple IoT objects at the device, network, application, and system levels. The $IDex_{System}$ evaluates the maturity of an IoT system or an integrated system comprised of a variety of objects at device, network, and application levels.

IDex is derived from a series of calculations, accounting for various criteria, extracted from the specification and data of an IoT object, and their weightings, indicating the importance level of each criterion. IDex is the weighted average of the criteria, providing an overall performance evaluation of IoT objects. With such an evaluation, the

development of large-scale IoT systems can be fostered from the aspect of system evaluation, ranking, and grading of IoT objects.

To showcase the use of IDex, we look into a case study of a scenario where developers are conducting a penetration test on a large-scale IoT system, taking Distributed Denial of Service (DDoS) attack, a common attack on IoT systems, as an example, the difference between the IDex of a system under normal operation and that of a system under a DDoS attack can indicate the impact of the attack on the system. Such measures can be taken into account in the analysis of the endurance of the system under attack. If DDoS defense modules are considered to be applied to the system, the differences between the IDex of the system under a DDoS attack with and without each defense module can reflect the effectiveness of each module, which can be taken into account in the determination of which defense module to be implemented to optimize the system. This scenario of utilizing the IDex will be shown in the demonstration session of INTEROP 2022.

Although the detail of IDex has not yet been defined, the requirements, categories, criteria, and mechanisms will be defined in the standard of IEEE P2668.1, which is under active development. Service-specified standards that will also be defined in the future by the P2668.10.X standards, tailored for specified services such as smart city, energy management, agriculture, aviation, etc [3].

III. Material and Equipment

The demonstration showcases IDex and its evaluation mechanisms. Materials and equipment used in the demonstration are (1) a LoRaWAN system implemented with an IDex monitoring module; (2) a DDoS attack module; (3) a firewall module.

IV. Demonstration

The demonstration is bisected into two phases, showcasing how IDex can evaluate the performance of an IoT system.

In phase 1, a LoRaWAN system will be implemented with selected smart applications for demonstration. With IDex real-time monitoring modules implemented, the IDex score of the system can be monitored. Here, the IDex of the system is defined as V1. Meanwhile, the DDoS attack module will be set up, targeting the LoRaWAN, or the LoRa Network Server explicitly. Upon being attacked, the LoRaWAN system will suffer a drop in performance, as the latency, packet loss rate, and data accuracy of the system are affected by the malicious traffic occupying the network capacity and computing power of the system. Therefore, the IDex of the system presented by the real-time monitoring model will drop. The IDex under the DDoS attack is defined as V2. In phase 2, a firewall module will be implemented in the system, protecting the network server from the attack of the DDoS attack module. As the effect of the DDoS attack on the system is mitigated, the performance will resurge under the implementation of the firewall module, which entails the resurgence of IDex, defined as V3, as shown in Figure 2.

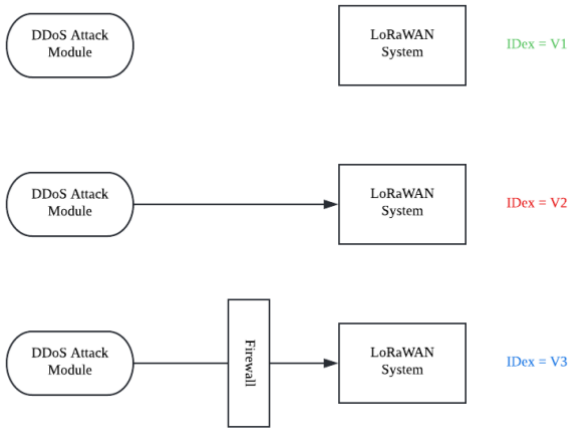


Fig. 2. Visual Representation of the Demonstration (V1>V2; V2<V3)

As IDex reflects the maturity of IoT systems, it can be used by developers for penetration tests, identifying the impact of an attack on a system (the drop from V1 to V2). The effects of different security measures on the system can also be evaluated quantitatively. For instance, in the demonstration, the addition of the firewall module entails the rise of IDex from V2 to V3, indicating that adding the firewall module will enhance the maturity of the system.

Acknowledgment

The support from the IEEE P2668 Standard Working Group is gratefully acknowledged.

References

[1] Zhu, Hong et al, "Index of Low-Power Wide Area Networks: A Ranking Solution toward Best Practice." IEEE Communications Magazine 59.4 (2021): 139-144.

[2] Y. Liu et al., "Multi-Layer IoT-DDoS Defense System Using Deep Reinforcement Learning," to appear in IEEE Transactions on Consumer Electronics.

[3] IEEE Standards Association. "P2668 - Standard for Maturity Index of Internet-of-things: Evaluation, Grading and Ranking." https://standards.ieee.org/project/2668.html (accessed September 30, 2022).