Advancing the Industrial Internet of Things

An Industrial Internet Consortium and oneM2M™ Joint Whitepaper

Authors

Amar Deol (Huawei), Ken Figueredo (InterDigital Inc.), Shi-Wan Lin (Yo-i), Brett Murphy (RTI), Dale Seed (Convida Wireless), Jason Yin (Huawei)

Editors

Shi-Wan Lin (Yo-i) and Ken Figueredo (InterDigital Inc.)

Contributors[1]

Josef Blanz (Qualcomm), Omar Elloumi (Nokia), Rajive Joshi (RTI), Peter Klement (XMPro), Sam Bhattarai (Toshiba), Atte Lansisalmi (Nokia) and Chuck Byers (IIC)

2019-12-12

[1] Individuals who have provided valuable comments and inputs that have substantially improved the quality of this whitepaper.

This white paper demonstrates how two leading organizations in the Internet of Things (IoT) can work together towards a common purpose of a robust, interoperable, flexible and efficient Industrial Internet of Things (IIoT). We first introduce the two organizations, the Industrial Internet Consortium (IIC) and oneM2M™, then illustrate their technical approach to IoT solutions, demonstrating how both organizations' thought leaders envision the growth of IoT through collaboration.

1 Context for Collaboration

Many in IoT recognize that few companies can provide complete solutions by themselves because many components and areas of expertise are involved. Consequently, collaboration among companies and organizations in the ecosystem is a necessary part of any IoT strategy.

Collaboration extends beyond technology and solution suppliers and users of IoT solutions. It applies also to standardization bodies and industry alliances. Several regional standards development organizations (SDOs) chose to collaborate in forming oneM2M[2] to develop and manage the technical standards to enable IoT solutions. The objective was to drive global scale in standards development and avoid standards balkanization.

Similarly, in consumer IoT, supplier-sponsored initiatives such as the AllSeen Alliance and the Open Connectivity Foundation merged their efforts into a single body representing a wider range of supplier interests. Another example is the merger of the IP for Smart Objects (IPSO) Alliance with the Open Mobile Alliance (OMA) with their joint focus on a communications stack, data model and device-management solutions for constrained IoT devices.

This paper provides some historical context on a liaison between oneM2M and IIC, explores areas of commonality between each other's work and identifies under-addressed technical areas and standardization gaps that, once resolved, would speed up the pace of commercial adoption for IoT solutions among providers and users alike. It builds on the discussion points covered in an inaugural meeting in February 2018, notably the respective histories and publications of each organization. It describes a comparative analysis between architecture frameworks and architecting methodology put forward in the IIC's Industrial Internet Reference Architecture (IIRA), oneM2M's architecture and its three-stage standardization procedure.

The commonalities discovered from this analysis set the stage for future collaboration to explore new requirements for interoperability across multiple dimensions including interworking between subsystems in factories, large machines and shared work environments (such as buildings, cities, logistics value-chains and transportation networks). We aim to share knowledge on replicable IIoT deployments and to leverage the IIC's well-run testbed program to identify new requirements and feed these into the oneM2M standardization and future-release roadmap.

[2] oneM2M: Standards for M2M and the IoT: *http://onem2m.org/*

2 ORGANIZATIONAL OVERVIEWS

The IIC and the oneM2M Partnership Project have distinct identities based on their origins and IoT market-development objectives. We briefly describe the history, structure and operating model for each organization, and reference key accomplishments, industry resources and plans for future initiatives.

2.1 OVERVIEW OF THE IIC

Founded in March 2014, the IIC is the world's leading organization that serves to transform business and society by accelerating the adoption of IIoT. It accomplishes this by enabling trustworthy industrial internet systems, where systems and devices are securely connected and controlled to deliver transformational outcomes across multiple industries. These industries include healthcare, transportation, energy, public domain infrastructures and manufacturing.

IIC's membership includes technology innovators, vertical market leaders, researchers, universities and government organizations. Its goals include:

- driving innovation through the creation of new industry use cases and testbeds for real-world applications,
- defining and developing the reference architecture and frameworks necessary for interoperability,
- providing inputs to and influencing the global development standards process for internet and industrial systems,
- facilitating an open forum to share and exchange real-world ideas, practices, lessons and insights and
- building confidence around innovative approaches to security.

IIC provides an environment for its members to connect with a global IIoT community and gain experience and foster partnerships. Clearly, the cross-pollination of activities benefits members directly and the industry at large.

The IIC has established a thriving testbed program in which the innovation and opportunities of the industrial internet—new technologies, new applications, new products, new services, new processes—can be initiated, thought through, and rigorously tested to ascertain their usefulness and viability before coming to market. The IIC has 26 active testbeds as of the date of this publication.

IIC members collaborate to deliver architectures, frameworks, requirements for standards and more. Since its founding, IIC has published a sequence of globally influential technical reports:

The *Business Strategy and Innovation Framework* (BSIF)[3] provides a high-level identification and analysis of issues that an enterprise needs to address to capitalize on the opportunities in IIoT.

[3] *https://www.iiconsortium.org/BSIF.htm*

The *Industrial Internet Reference Architecture* (IIRA)[4] is a blueprint for building industrial internet systems. It outlines a standards-based open-architecture framework template and methodology for designing an IIoT system.

The *Industrial Internet Security Framework* (IISF)[5] provides guidance on IIoT security. It uses the concept of *trustworthiness* to address the entwined nature of security, safety, reliability, resilience and privacy in IIoT systems and communities.

The *Industrial Internet Connectivity Framework* (IICF)[6] provides a comprehensive treatment of connectivity as a means of building interoperable IIoT systems.

The *Industrial IoT Analytics Framework* (IIAF)[7] outlines requirements and concerns for analytics for IIoT systems and recommendations for meeting the requirments and addressing them.

The *Industrial Internet Vocabulary Technical Report*[8] specifies a common set of definitions for effective communication within the industrial internet ecosystem.

At the end of 2018, the IIC joined forces with the OpenFog Consortium (OFC) to advance edge computing in IoT deployments. IIC also collaborates with major IIoT-related organizations including standards organizations, open-source organizations, other consortia and alliances (either technology- or industry-focused), certification and testing bodies and government entities or agencies through its liaison programs. One of these is with oneM2M. IIC currently has 52 liaison relationships globally.

An example outcome from these collaborations include the IIC and Plattform Industrie 4.0[9] jointly published *Architecture Alignment and Interoperability: An Industrial Internet Consortium and Plattform Industrie 4.0 Joint Whitepaper*, which details the mapping and alignment between the two leading IIoT reference architecture models, the IIRA and the Reference Architecture Model for Industrie 4.0 (RAMI 4.0).[10]

This IIC and oneM2M joint whitepaper is another example of a successful collaboration.

2.2 Overview of oneM2M™

oneM2M brings together several major ICT SDOs around the world, such as ARIB (Japan), ATIS (North America), CCSA (China), ETSI (Europe), TIA (North America), TSDSI (India), TTA (S. Korea)

---

[4] http://www.iiconsortium.org/IIRA.htm

[5] https://www.iiconsortium.org/IISF.htm

[6] *https://www.iiconsortium.org/IICF.htm*

[7] *https://www.iiconsortium.org/industrial-analytics.htm*

[8] *https://www.iiconsortium.org/vocab*

[9] Industrie 4.0 describes the combination of production methods with state-of-the-art information and communication technology, while Plattform Industrie 4.0 is the German cross-industry and government initiative to support the implementation of Industrie 4.0. (*http://www.plattform-i40.de/I40/Navigation/EN/Home/home.html*).

[10] *https://www.vdi.de/fileadmin/vdi_de/redakteur_dateien/gma_dateien/5305_Publikation_GMA_Status_Report_ZVEI_Reference_Architecture_Model.pdf*

and TTC (Japan).[11] These SDOs, referred to as "Partners Type 1", share the objective of developing common standards for a common service layer that applies across different industry segments.

The Partners Type 1 have acted strategically to achieve a much-needed convergence in the IoT standards landscape. Instead of developing IoT standards individually and for their local markets, they agreed, in 2012, to collaborate through the oneM2M partnership project. To promote oneM2M, they facilitate the development and publication of oneM2M specifications as their own standards.[12] This ensures a global and institutional reach for oneM2M. In 2018, the ITU formally adopted the oneM2M specifications, including a full international recommendation[13] for the oneM2M architecture.

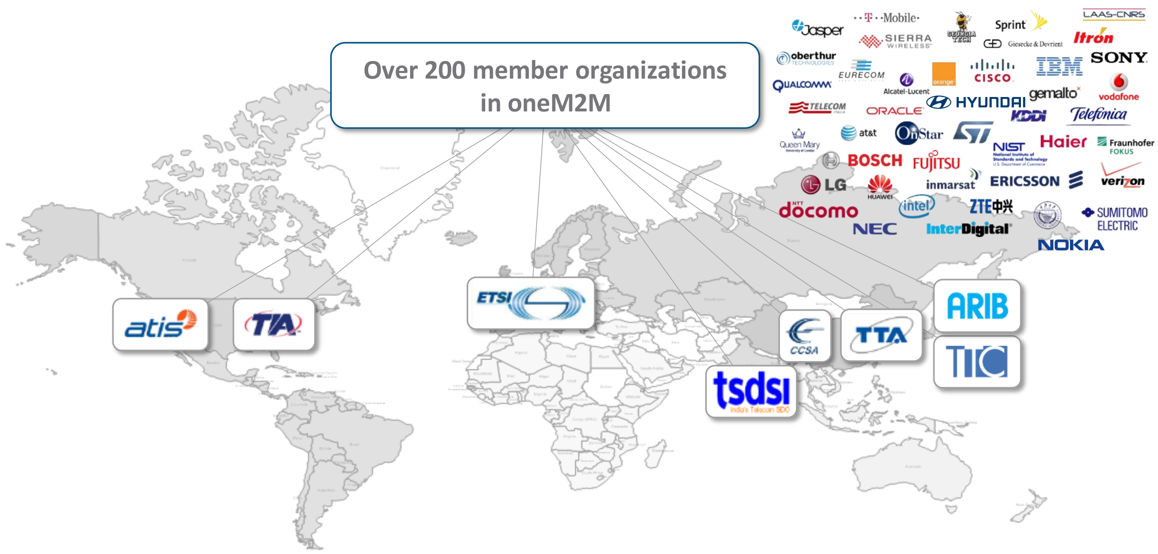

Figure 1 oneM2M member organizations (Source: oneM2M)

Currently, there are 200 active members in oneM2M. All share the vision of specifying a common service layer, a layer that sits between applications and networks and exposes functions needed by IoT applications across different industry segments.

Several fora and industry alliances working on IoT-related topics also joined oneM2M. They play an important role in shaping oneM2M specifications and ensuring a coordinated approach. These

[11] *ARIB - Association of Radio Industries and Businesses - www.arib.or.jp/english/arib/about_arib.html*
ATIS - Alliance for Telecommunications Industry Solutions - www.atis.org
CCSA - China Communications Standards Association - www.ccsa.org.cn/english/
ETSI - European Telecommunications Standards Institute - www.etsi.org/
TIA - Telecommunications Industry Association - www.tiaonline.org/
TSDSI - Telecommunications Standards Development Society, India - www.tsdsi.in/
TTA - Telecommunications Technology Association - www.tta.or.kr/English/
TTC - Telecommunication Technology Committee - https://www.ttc.or.jp/e/index.html

[12] oneM2M latest specification drafts *http://onem2m.org/technical/published-drafts*

[13] *ITU-T Publication Y.4500.1 : oneM2M Functional Architecture - https://www.itu.int/rec/T-REC-Y.4500.1/en*

are referred to as Partners Type 2, and the category presently includes GlobalPlatform, which creates and publishes an international standard for enabling digital services and devices to be trusted and managed securely throughout their lifecycle.

The process of developing oneM2M specifications is open and contribution-driven, as distinct from proprietary approaches. This means that the industry at large can influence the direction of the specifications and market deployments. Moreover, oneM2M maintains liaisons with other standards initiatives and industry fora, such as the IIC and Plattform Industrie 4.0, to ensure complementary approaches.

Architecturally, oneM2M's common service layer functions as a horizontal, abstraction layer between IoT applications (i.e. business logic) and the communications networks that provide connectivity to end-point devices and sensors (i.e. actuation and data capture). The benefit of this abstraction layer is that users of the oneM2M specifications do not need to master integrated stack technologies to design, deploy and manage multiple IoT applications or IoT applications in different industry verticals.

The common service layer offers a set of common service functions, e.g. device management, registration and security. It horizontally joins the middle layers of several separate, heterogenous, vertical IoT solutions. The sharing of common capabilities at this middle layer ensures re-usability and delivers economies of scale.

Another aspect of oneM2M's horizontal architecture is that it lays the foundations for cross-silo interoperability. Individual IoT solutions can share data and resources through common service layer functions such as resource discovery and semantic interoperability. As a result, application developers, solution providers and data suppliers can share data between application silos and reduce their dependence on single-vendor solutions.

oneM2M follows a use-case-driven approach to IoT standardization with real-world scenarios that serve to derive requirements for the common service layer. By doing so, it can address the needs of multiple use cases including the ones that the group did not anticipate at the time of the specification, thus building an element of future-proofing in the standardization process.

To enhance the stability of the oneM2M specifications and shorten time to market, oneM2M hosts multiple interoperability and hack-a-thon events every year. Engineers can test their products against each other, in accordance with agreed test specifications, and participants can learn more about oneM2M. These events are a significant asset in validating oneM2M's technical specifications and their implementation across multiple solution providers.

In addition, the Global Certification Forum (GCF) manages a oneM2M global certification program.[14] oneM2M certification through GCF ensures oneM2M solution providers maintain the

[14] *GCF and TTA officially sign agreement for oneM2M global certification solution at MWC19 https://www.globalcertificationforum.org/news/gcf-tta-sign-onem2m--agreement-at-mwc19.html*

proper functionality and compliance with the oneM2M specifications and that oneM2M solutions can interoperate with one another.

The full suite of oneM2M[15] technical specifications, including different releases, is available for download at *www.oneM2M.org*.

3 Alignment Between IIRA and oneM2M Architecture Frameworks

Emphasizing cross-industry versatility and interoperability, the IIRA and its companion documents provide a framework and a methodology for business-value-driven system design. It recognizes that data analytics and AI plays an essential role in enabling end-to-end optimization of connected industrial systems from equipment to enterprise information systems. Its broad applicability provides a common foundation for industries to communicate important shared architectural concerns and solutions to address them. As a common blueprint for designing specific architectures, it enables interoperability and encourages reusability of IIoT technologies across industrial sectors.

oneM2M technical specifications address the need for a common service layer for Machine-to-Machine (M2M) and IoT applications, across different vertical domains, via a horizontal platform architecture. oneM2M's three-layer architecture comprises applications, a common services layer (middleware) and networks. oneM2M standardizes the interfaces between these layers. This provides a secure means for connecting data 'producers' and data 'consumers'. By abstracting complex interfaces, oneM2M aims to simplify life for application developers. The applicability of oneM2M specifications to different vertical domains enables interoperability between applications and connected devices as well as across application and organizational silos.

Despite their different origins and approaches in addressing IoT and IIoT architectural challenges, IIC and oneM2M share common objectives in helping industries achieve interoperability and reusability. They share a common goal of reducing the complexity and the cost of designing, developing and deploying IoT and IIoT systems, shortening the time-to-market and time-to-value-creation cycles.

The IIRA and oneM2M architectures build on largely the same technological foundations: a new set of communication connectivity technologies (e.g. web and RESTful services, Data Distribution Service (DDS), OPC UA) and computational technologies, (e.g. cloud computing, big data and machine learning). Consequently, they share several architectural elements that map to each other; there are also differences in focus and approach. We next analyze those commonalities and differences, then discuss their architectural complementarity along with recommendations on how to best leverage the strength of each in conceptualizing IIoT systems.

[15] *The term "oneM2M" can refer to the organization that develops the oneM2M standard and to the standard per se.*

3.1 IIC's IIRA

The IIRA provides a high-level architectural framework and methodology that enables rapid realization of interoperable IIoT systems. It provides guidance for their development by identifying and highlighting important architectural concerns, concepts and patterns that can be applied within and across industrial sectors. Interoperability issues within and across IIoT systems can be identified and resolved for the broadest set of IIoT applications.

Technology vendors can use the IIRA concepts and methodology to build interoperable system components that address the broadest possible market. System implementers can use the IIRA as a starting point to shorten system development by deploying reusable, commercially available, or open-source system building blocks to reduce project risk, associated costs, and time-to-market. It is applicable to almost all industrial sectors, including manufacturing, transportation, energy, agriculture, healthcare and public infrastructure. Ultimately, the IIRA helps reduce the cost of design and operations by creating a community with a common language.

The structure of the IIRA contains architectural concepts, vocabulary, structures, patterns and a methodology to address important common architectural concerns. It defines an architecture framework through a carefully defined standards-based framework and common terminology by adapting architectural concepts, constructs and approaches from the ISO/IEC/IEEE 42010-2011 Systems and Software Engineering—Architecture Description[16] standard. The IIRA clarifies how this framework is used to create the content of the reference architecture itself and how the reference architecture is to be applied to create concrete IIoT architectures.

Architectural concerns are identified and classified into four viewpoints, per the ISO/IEC/IEEE 42010-2011 Systems and Software Engineering—Architecture Description, then the concerns are analyzed systematically and resolved (see *Figure 2*). The results are documented in models and other representations in the respective view as the content of the architecture description.

Those viewpoints are:

The *business viewpoint* identifies stakeholders and their business vision, value and objectives of an IIoT system.

The *usage viewpoint* describes how the IIoT system is expected to be used to deliver the intended business objectives.

The *functional viewpoint* focuses on the functional components and the structure in which they are interrelated and interact with each other and with external elements in the environment in such a way as to support the intended usages.

[16] ISO/IEC/IEEE: "ISO/IEC/IEEE 42010:2011 Systems and software engineering -- Architecture description", 2011, *http://www.iso.org/iso/catalogue_detail.htm?csnumber=50508*

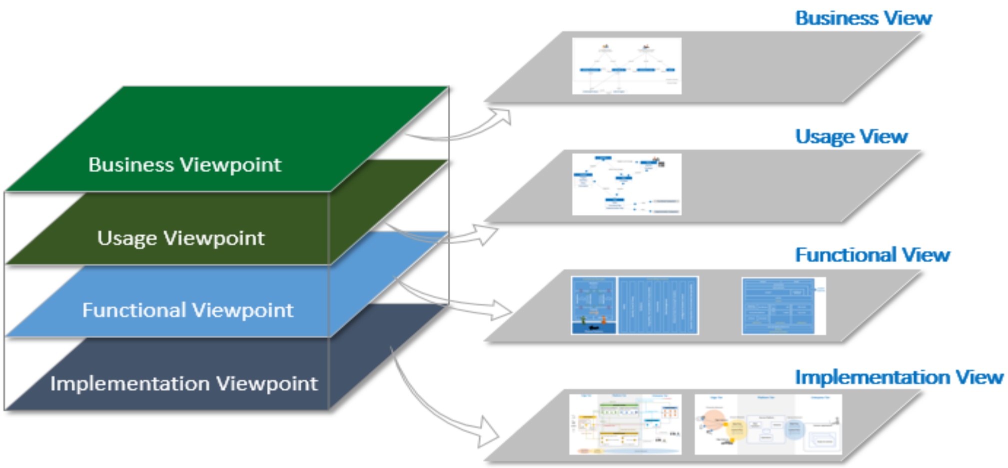

Figure 2 IIRA Architecture viewpoints and views

The *implementation viewpoint* determines the technologies needed to implement functional components, their communication schemes and their lifecycle procedures.

The IIRA offers a comprehensive system analysis in each of the viewpoints. For example, business decision-makers, plant managers and IT managers can use the business viewpoint to help them better understand how to drive IIoT system development from a business perspective.

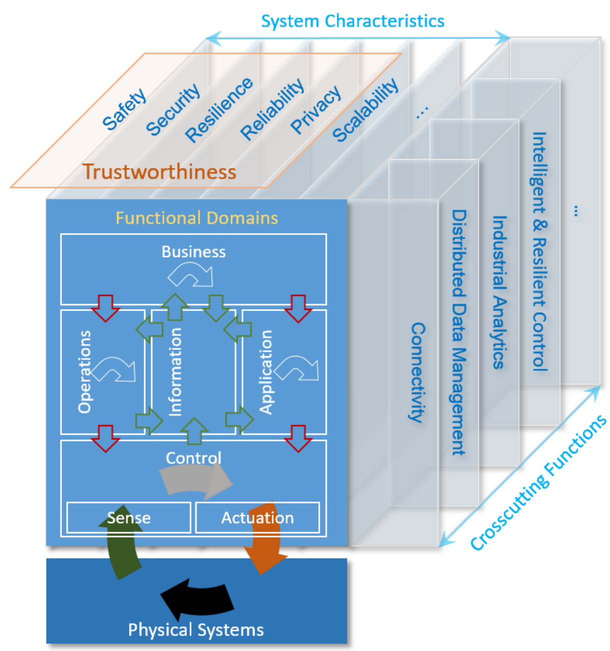

Figure 3 Functional domains, crosscutting functions and system characteristics

For another, the functional viewpoint defines the functional domains (*Figure 3*) that are most important to consider in an IIoT system and clarifies the concepts and relationship between them and the crosscutting functions that need to be made available across many of the system functional components.

For example, system functions need to be connected so they can interact with each other to complete functionality at the system level. Therefore, connectivity is considered a crosscutting function.

The IIRA also defines the concept of system characteristics as system properties and behaviors of an IIoT system resulting from those of its constituent sub-systems and the nature of their interactions with each other, the context and the environment in which they operate. An example of important system characteristics is *trustworthiness*, which encompasses safety, security, privacy, reliability and resilience—a concept well developed in the IISF. It also examines how the IIRA functional domains map to a deployment continuum ranging from edge to cloud to reflect the latest thinking in IIoT architecture.

The IIRA is incrementally aggregating knowledge and guidance as technologies develop, and successful best practices are described.

3.2 oneM2M Architecture and Common Services Layer

Many IoT applications are deployed as silos in a vertical solution stack. At its simplest, this involves one application (e.g. asset tracking, condition monitoring, inventory tracking logic) using one communications network to interact with connected devices or sensors.

This arrangement does not lend itself to operational scaling or resource reuse. Consider an IoT application that requires a device management capability, for example. If the device management function is implemented for a narrowly defined use case this could easily prevent its reuse for a second or third IoT application. The same logic applies to other service enablers necessary for the deployment and management of IoT applications.

To solve the problem, the oneM2M architecture applies a horizontal model based on a common services framework. Examples of common services include communications management, device management and security functions. The architecture also means that devices and their data are both discoverable and accessible to more than a single parent application.

Applications can be built using oneM2M-capable devices sourced from multiple suppliers, reducing the risk of vendor lock-in. This allows solution providers to build only once and reuse many times. This is a significant advantage when a lack of standardization inhibits permutations across multiple technology vendors, service providers, organizational boundaries and IoT applications.

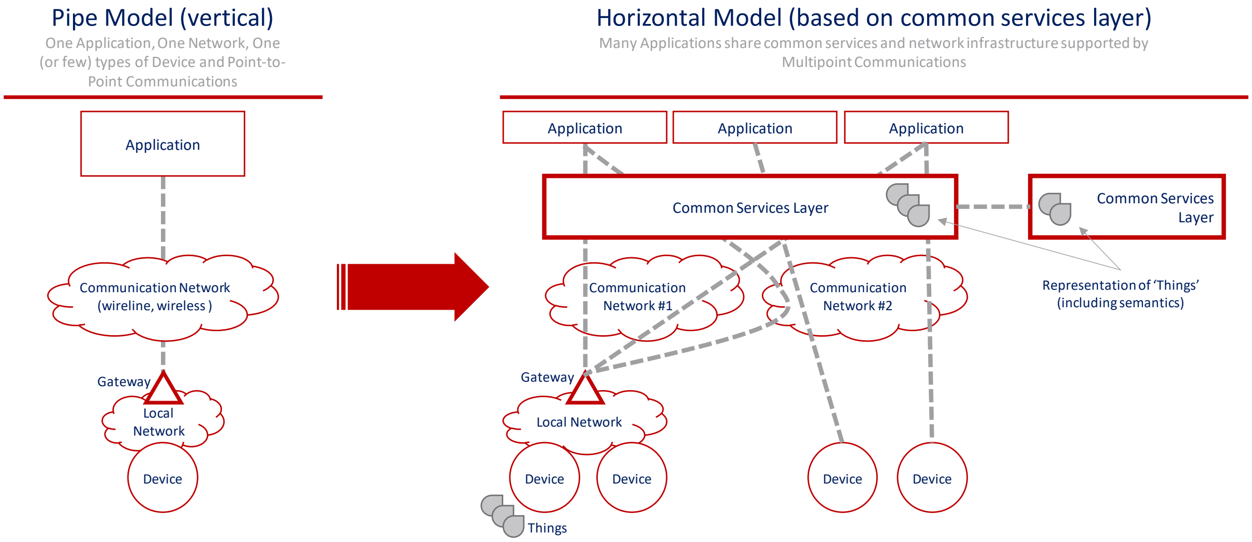

Figure 4 Overview of oneM2M Horizontal Architecture (Source: oneM2M)

In addition to standardizing the common services layer, oneM2M includes specifications for end-device and gateway entities. This makes it possible to deploy native-oneM2M solutions, comprising oneM2M compliant end-devices communicating with one or more oneM2M platforms. It is also possible to cater for deployments that contain a mix of oneM2M and proprietary devices. This involves the use of an interworking proxy gateway to manage non-oneM2M devices communicating with a oneM2M platform.

The oneM2M standards are a horizontal common services layer IoT platform that allows applications within a domain (e.g. a city, factory or transportation hub) to communicate effectively, reliably and securely. The standard supports a federated model of operation so that these benefits accrue to applications from various previously siloed domains (e.g. to manage transportation and environmental sensing on road networks or, utilities and wellness in offices and households).

3.2.1 Common Service Layer Functions

From a functional perspective, oneM2M has defined fourteen common service functions (CSFs). These relate to network connectivity, device security, transport protocols, content serialization, IoT device services and management and IoT semantic ontologies.

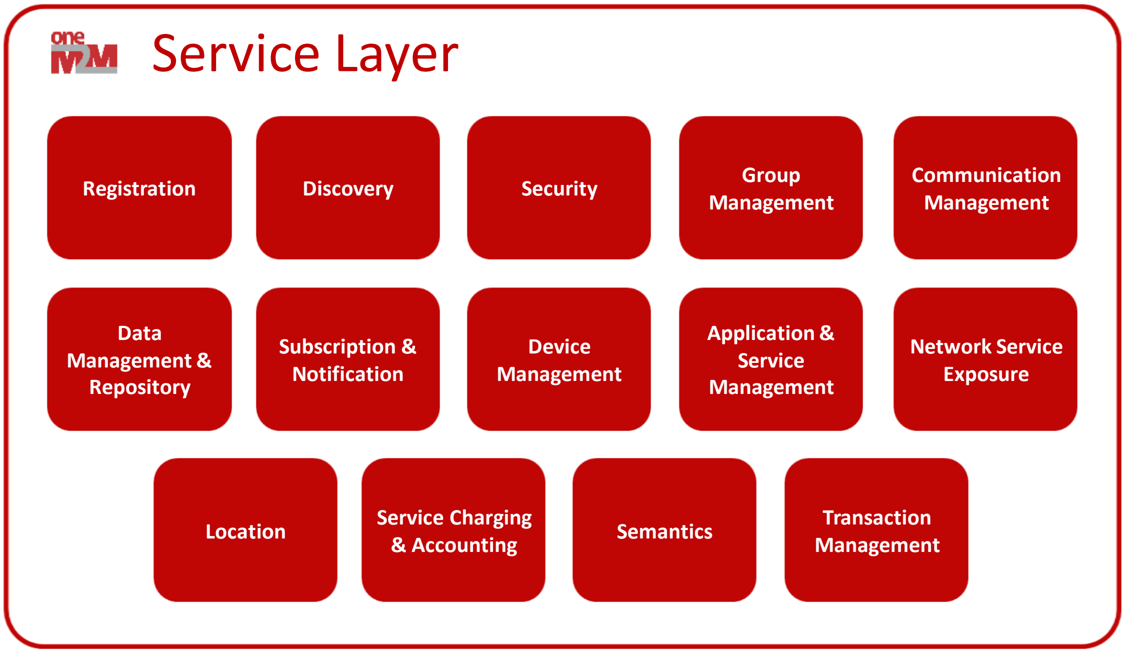

Figure 5 oneM2M Common Service Layer Functions (Source: oneM2M)

Each of these oneM2M services lets application developers focus on application-specific functionality (e.g. turning a switch on or off), while relying on abstraction techniques to mask the underlying technology-specific details, by allowing bindings to different communications stacks and protocols such as HTTP, CoAP and MQTT. For example, the switch might use a fixed or Wi-Fi network, a CoAP or HTTP transport. It might use a JSON or XML serialization technique, an Open Connectivity Foundation (OCF) or thread service enablement, or an ontology based on Smart Appliances REFerence (SAREF) or W3C's Thing Description.

Finer-grained capabilities underpin each service function as illustrated in the case of device management, security and application and service management functions.

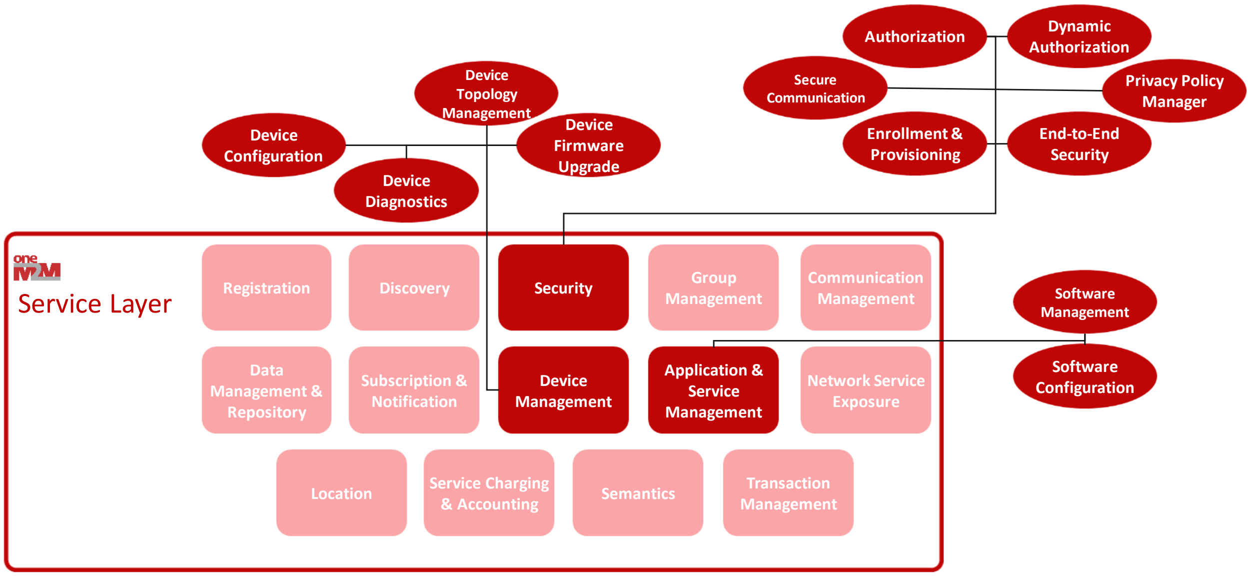

Figure 6 Illustrative Features of oneM2M Common Service Layer Functions (Source: oneM2M)

In keeping with a philosophy of leveraging existing standards rather than re-inventing them, oneM2M complements existing and proven security technologies to address IoT security challenges. It provides a common set of security capabilities to secure IoT devices and applications and prevent and mitigate attacks. This is made possible by an abstracted set of security-related APIs to simplify security for devices and applications.

oneM2M is a constantly evolving standard with a strategic roadmap designed to address new IoT requirements. This is made possible by the common service layer concept, which was conceived to accommodate new service functions.

oneM2M works to a release cycle to standardize new service functions. It emulates the cellular industry's 3GPP standardization model, to address new requirements and evolving technologies through progressive releases.

3.3 Mapping Between IIRA and oneM2M

The IIRA decomposes the core functions of an IIoT system into functional domains and crosscutting functions, as illustrated in *Figure 3*. The functional domains focus on major system functions that are generally required to support generic IIoT usages and to realize generic IIoT system capabilities. The crosscutting functions need to be made available across many of the system functional components.

The crosscutting design approach is central to oneM2M technical standards. They underpin a software framework for linking IoT applications to a set of value-added services relating to: network connectivity, device security, transport protocols, content serialization, IoT device services and management and IoT semantic ontologies. These set of services let application developers focus on application-specific functionality (e.g. turning a light switch on or off) by abstracting out the complexity and heterogeneousness of the underlying technologies. They allow IoT developers to interact with diverse IoT devices and technologies from various vendors without the risk of locking into a single technology or single-vendor solution. All of these value-added services are provided in the common services layer, as shown in *Figure 4*.

From the functional point of view, the IIRA functional domains (*Figure 3*) can be mapped to the high-level functions in the oneM2M horizontal architecture (*Figure 4*). This mapping is depicted in *Figure 7*.

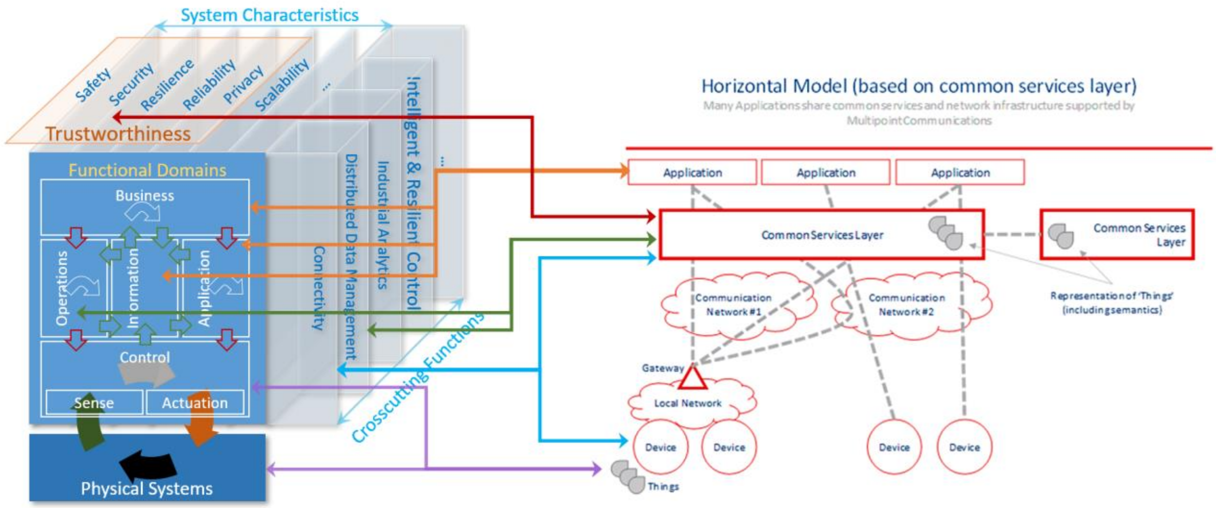

Figure 7 IIRA functional domain and oneM2M high-level service mapping

Here is a more detailed functional mapping of the oneM2M common service layer functions (*Figure 5*).

- Functions in the business, information and application domains, along with cross-cutting functions industrial analytics and intelligent and resillent control (neither has mapping lines) in the IIRA are considered functions in the oneM2M Application layer.
- The security functions considered in the IIRA System Characteristics corresponds to the security function in the oneM2M service layer.
- Functions in the operations domain and in the distributed data management in the crosscutting functions in the IIRA map to functions in the oneM2M common services layer. Specificically, functions in the IIRA operations domain map to registration, discovery, device management in oneM2M common services layer. Functions belong to the IIRA distributed data management map to the oneM2M data management and repository.
- Functions in the connectivity in the crosscutting function in the IIRA map broadly in both the common services layer and the devices (layer) across the network spans in the oneM2M horizontal achitectue. The IIRA connectivity functions directly map to

semantics, communication management, network service exposure and transaction management.

- Functions in the control domain and the physical systems in the IIRA map to those belonging to things in the one M2M horizontal layer).
- Other functions in the oneM2M services layer not mentioned above may not be described directly in the IIRA or they belong to its lower layer functions.

A common IIRA architecture pattern as described in its implementation viewpoint consists of solution elements arranged in three tiers—edge, platform and enterprise. In the illustration below, the edge tier comprises an edge gateway communicating with three devices via a proximity network. Another example of an edge tier capability is an edge gateway that aggregates data from connected sensors and data sources in a vehicle. The edge tier interacts with platform tier components via an access network. Data and control pathways are completed via a service network that links the platform and enterprise tiers.

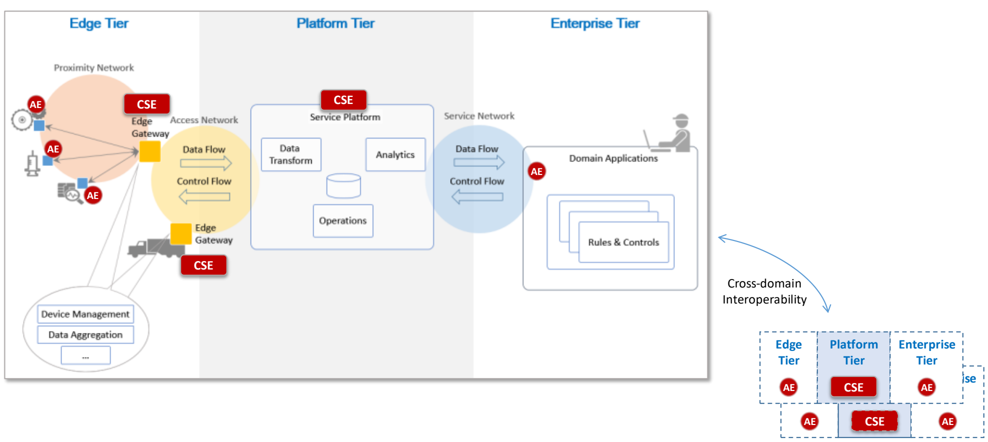

Figure 8 IIRA 3-tier architecture pattern mapping to oneM2M architecture elements

The latter contains domain applications such as asset tracking or condition monitoring, for example, and a user interface.

Superimposed in this illustration are oneM2M implementation components. There is an Application Entity (AE) for each connected sensor and data source. AEs implement a standardized application service logic within individual devices, gateways and sensors. AEs provide a standardized interface to manage and interact with applications.

The implementation of oneM2M's common services layer resides in Common Services Entities (CSEs), in a distributed architecture. Each CSE represents an instantiation of oneM2M's common service functions. It is feasible to embed CSE functionality in a gateway to place common services closer to the edge of an IoT deployment. A complex IoT deployment may involve several gateway CSEs interoperating with a cloud-based CSE, such as the one mapped onto the IIRA platform tier.

Among other features, CSEs control when communications occur, accounting for the time-sensitivity of communications and the economics of data transfer. For example, in non-time-critical applications, it is possible to accumulate data for efficient transfer at a later time. This may be especially relevant where power consumption is an operational priority.

To complete the solution chain, there finally needs to be an AE for the domain application in the enterprise tier, allowing it to interact with its associated edge devices and sensors.

The use of oneM2M AEs and CSEs provides a standardized way for devices and sensors to function in a network-agnostic manner with their associated domain applications. It hides the complexity and heterogeneity of network usage from applications, thus simplifying the implementation burden for application developers. To achieve this, it takes account of the specific capabilities and constraints of each available underlying network (fiber, satellite, cellular, proximal wireless, etc.) and makes the best use of them in the context of higher layer application needs. A configurable policy manger allows designers to define which applications and users can access which devices and sensors, making it possible to share data across application silos.

The main portion of the illustration above focuses on a single application. However, the distributed use of oneM2M elements means that multiple three-tier architecture implementations can interact with one another. Thus, a domain application in one deployment can discover and interact with a connected device or sensor associated with other applications.

3.4 Summary of Archecture Approaches and Alignment

The IIRA defines a standards-based architecture framework template and methodology that identifies and highlights common and important architectural concerns, concepts and patterns, that can be applied within and across different industrial sectors. Viewpoints make it a business-value-driven, concern-resolution architecting framework to design end-to-end IIoT system architectures across industrial verticals.

oneM2M is a global standard that defines a common service layer implementing a set of common services required by IoT systems, irrespective of the industry domain in which it is applied. These services abstract and isolate technology complexities for IoT application developers letting them focus on building, deploying and commercializing their applications.

The business viewpoint is a unique consideration in the IIRA not commonly found in IIoT architecture constructs, including oneM2M. IIoT designers who leverage the oneM2M common service layer may benefit from the analysis of business concerns as described in the IIRA business viewpoint.

From a functional perspective, the IIRA functional viewpoint describes functional domain and crosscutting functions covering IIoT systems end-to-end, while oneM2M defines a set of functions common across industrial verticals as middle layer services that hide the complexity in the devices layers and bridge the applications to the devices through service abstraction.

From an implementation point of view, there are ample synergies in the functional definition between the IIRA and oneM2M. System developers can follow the IIRA methodology and architecture patterns and use the oneM2M common service to support the architecture patterns. For those functional components that are not covered by the oneM2M common service layer, they can be naturally considered as application layer components in oneM2M and developed for the specific IIoT system. The set of oneM2M common services can be shared by different industrial verticals, enabling interoperability across these verticals, which is a goal that the IIRA also strongly seeks.

From a system-usage analysis perspective, the IIRA usage viewpoint provides a way to analyze how the system is to be used to achieve its objectives. A oneM2M use case describes who is to use the system, and how to benefit from the system. A oneM2M use case is therefore an instantiation of an IIRA usage viewpoint.

4 Convergence and Interworking

The introduction of machine-to-machine solutions into industrial IoT applications is progressing in three phases. In the past, industrial control systems typically employed a master/slave architecture. Currently, many local IoT applications on factory floors and in complex machines are linking multiple proximal networks through cloud-based data aggregation and supervisory control systems. But now, as the IoT market matures across consumer and industrial sectors, IoT applications will employ distributed architectures. Moreover, as large-scale deployments and interoperability (e.g. cross-vendor, cross-silo, cross-organizational) become necessary, solution architectures will depend on new and standardized enablers that interlink multiple sub-systems to peers and to central cloud systems.

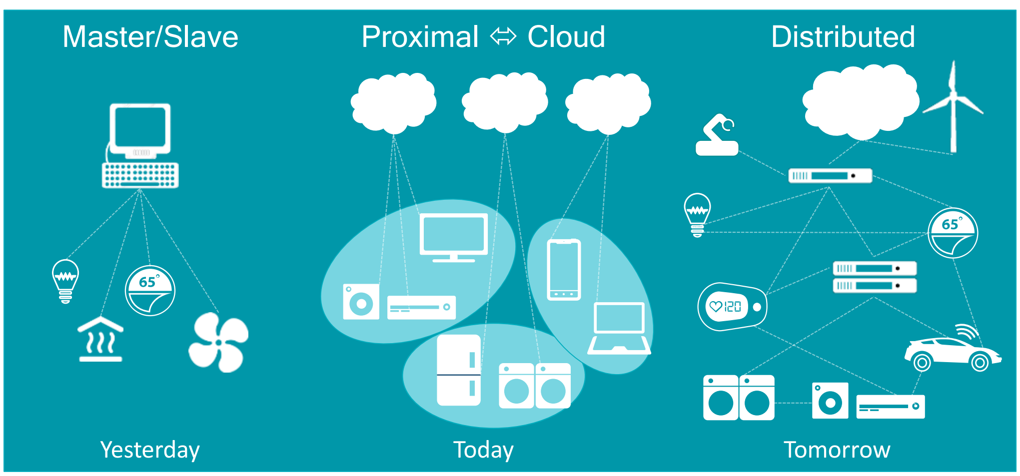

Figure 9 Trends in the evolution of M2M to IoT (Source: oneM2M)

The IIC developed the Industrial Internet Connectivity Framework to provide guidance and best practices for developing IIoT systems with interoperability between applications, subsystems and devices across a distributed, interworked system of systems. It describes a connectivity reference architecture to address this interoperability challenge, as illustrated below.

Fundamental to the successful use of the connectivity reference architecture is selecting a core connectivity standard to bridge applications and devices in an IIoT system. The IICF identifies potential core connectivity standards and provides detailed assessment templates to evaluate connectivity technologies so that an IIoT system can choose a core connectivity standard that best aligns with its connectivity needs.

To qualify as a core connectivity standard, there must be standard mappings (i.e. bridges) to the other core connectivity standards as referred in the IICF. Interoperability between subsystems using different core connectivity standards is provided via core gateways that implement these standard mappings. This limits the number of core connectivity standards, reducing complexity, while still covering the needs of IIoT systems across both functional domains and industries.

The gateway functions described above may be simple bridges converting data and protocols between connectivity core standards, or they may include more complex edge computing functions. Edge processors can perform analytics, data reduction, artificial intelligence, machine learning, security processing, storage and many other functions. They not only convert between core connectivity standards, but also beneficially process the data as it passes through the gateway functions.

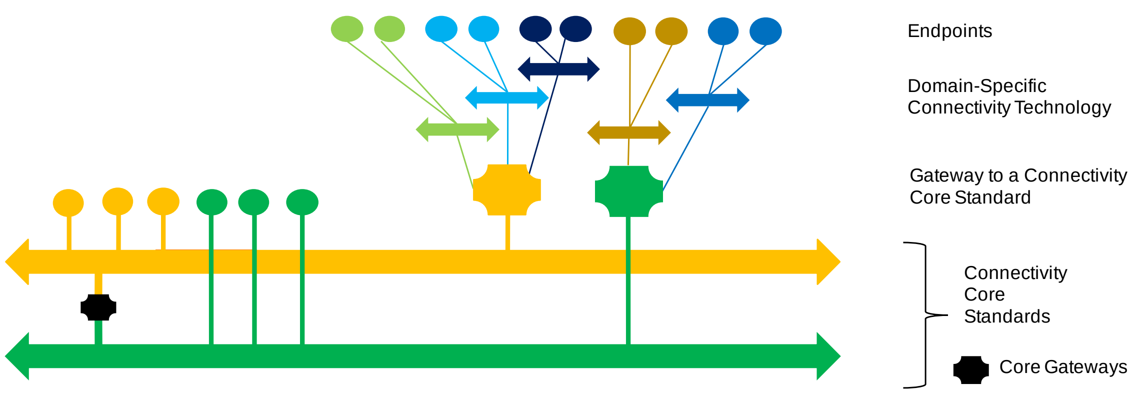

Figure 10 Standardized gateway for end-point interoperability (Source: IIC IICF)

The IICF recommends that system architects select a framework-layer standard for core connectivity. A framework-layer standard (e.g. DDS, OPC-UA, Web and RESTful Services) provides syntactic interoperability, i.e. the ability to exchange data. It standardizes the format of the data being communicated and how that data should be communicated and provides more data handling and communication management capabilities over lower-level transport-layer standards (e.g. MQTT, CoAP, HTTP). The IICF provides detailed assessments of several framework-and transport-layer standards to help system architects choose the best connectivity technology for their needs.

The IICF addresses syntactic interoperability, but not the data or information model standards needed to address what the data means, or its context (is it a temperature or a pressure measurement?) i.e. semantic interoperability. The IIC is working on information model guidance for future publication. oneM2M, however, currently addresses the need for standard information models and bridging or translating between different framework layer standards.

The standardization roadmap for oneM2M envisages providing a protocol abstraction layer on top of multiple connectivity technologies. It will complement and interwork various proximal industrial communication technologies (e.g. DDS, OPC-UA, WirelessHART, IWLAN) to the broader internet.

This permits the use of established standards from the fixed-network, mobile-network and internet sectors (left-hand side of illustration) to be applied in support of applications from the industrial sector, smart homes and eHealth, for example. It maximizes the re-use of established industry standards.

The following lists cross-industry and industry-specific protocols that oneM2M supports or plans to support.

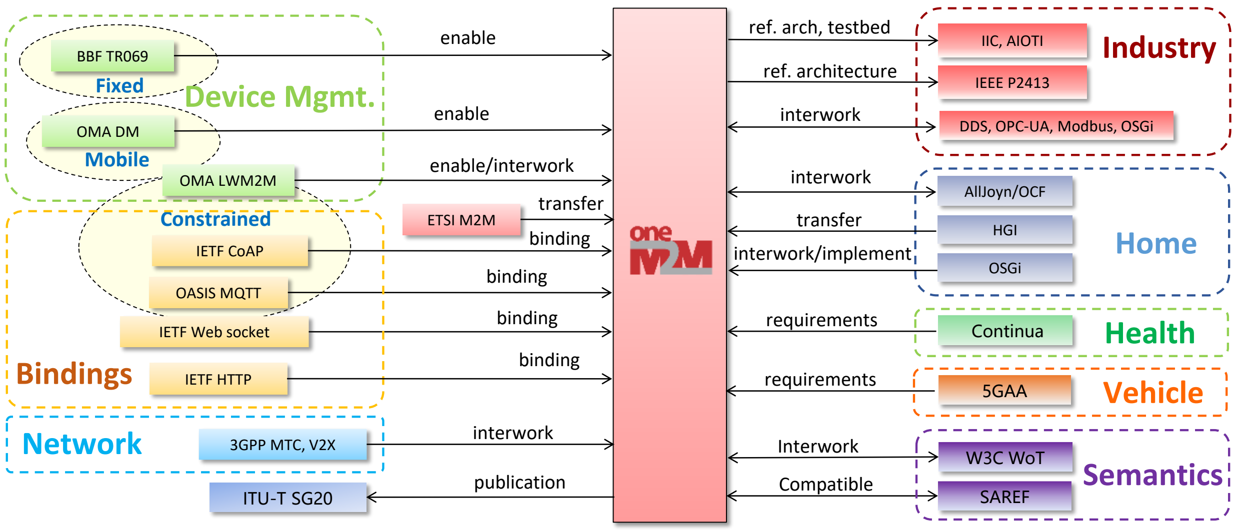

Figure 11 oneM2M role as an interoperability hub across industries and industry-specific protocols (Source: oneM2M)

BBF TR069	Techical specification of the Broadband Forum that defines an application layer protocol for remote management of customer-premises equipment connected to an Internet Protocol network	https://www.broadband-forum.org/resources?resource_tags=tr-069
OMA DM	Device management protocol specified by the Open Mobile Alliance (OMA)	http://openmobilealliance.org/wp/index.html
OMA LWM2M	Lightweight M2M is a protocol from the Open Mobile Alliance for M2M or IoT device management.	http://openmobilealliance.org/wp/index.html
IETF CoAP	Constrained Application Protocol (CoAP) is a specialized web transfer protocol for use with constrained nodes and constrained (e.g., low-power, lossy) networks	https://tools.ietf.org/html/rfc7252
OASIS MQTT	Lightweight publish/subscribe reliable messaging transport protocol suitable for communication in M2M/IoT contexts where a small code footprint is required and/or network bandwidth is at a premium	https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=mqtt
IETF Web Socket	The WebSocket Protocol enables two-way communication between a client running untrusted code	https://tools.ietf.org/html/rfc6455

	in a controlled environment to a remote host that has opted-in to communications from that code.	
IETF HTTP	The Hypertext Transfer Protocol (HTTP) is an application-level protocol for distributed, collaborative, hypermedia information systems.	https://tools.ietf.org/html/rfc2616
3GPP MTC, V2X	3GPP family of wireless communication technologies that include specific support e.g. for V LTE support of Vehicle-to-Everything (V2X) services and, for Machine-Type Communications (MTC)	https://www.3gpp.org/specifications
ITU-T SG20	ITU-T Study Group 20: IoT, smart cities and communities	https://www.itu.int/en/ITU-T/about/groups/Pages/sg20.aspx
AIOTI	Alliance for Internet of Things Innovation	https://aioti.eu/
IEEE P2413	IEEE Draft Standard for an Architectural Framework for the IoT	https://standards.ieee.org/project/2413.html
DDS	Data Distribution Service (DDS) for real-time systems is an Object Management Group M2M standard for scalable, real-time, dependable, high-performance and interoperable data exchanges using a publish–subscribe pattern	https://www.omg.org/spec/DDS/1.0
OPC-UA	OPC Unified Architecture is a machine to machine communication protocol for industrial automation developed by the OPC Foundation.	https://opcfoundation.org/developer-tools/specifications-unified-architecture
Modbus	Modbus is a serial communications protocol that has become a *de facto* standard communication protocol for connecting industrial electronic devices.	http://modbus.org/specs.php
OSGi	The OSGi Alliance is a worldwide consortium of technology innovators that advances a proven and mature process to create open specifications that enable the modular assembly of software built with Java technology	https://www.osgi.org/about-us/
Alljoyn/OCF	Open source software framework that makes it easy for devices and apps to discover and communicate with each other	https://openconnectivity.org/
HGI	The Home Gateway Initiative is nonprofit trade organization to discuss the key specifications and standards of residential gateways, also known as home gateways	http://www.homegatewayinitiative.org/
Continua	Continua Design Guidelines specify an end-to-end ICT framework for personal connected health solutions based on recognized open standards	https://www.pchalliance.org/about-continua
5GAA	The 5G Automotive Association (5GAA) is a global, cross-industry organisation of companies from the automotive, technology, and telecommunications industries (ICT), working together to develop end-to-end solutions for future mobility and transportation services	http://5gaa.org/about-5gaa/about-us/
W3C WoT	W3C's Web of Things Working Group aims to develop initial standards for the Web of Things, with the goals of countering IoT fragmentation; reducing development costs; lessening investor and customer riskss; and encouraging exponential growth in the market for IoT devices and services.	https://www.w3.org/WoT/

SAREF	The Smart Appliances REFerence (SAREF) ontology is a shared model of consensus that facilitates the matching of existing assets (standards/protocols/datamodels/etc.) in the smart appliances domain	https://sites.google.com/site/smartappliancesproject/home

5 FUTURE DIRECTIONS

In light of their respective organizational goals, the IIC and oneM2M will continue to foster the development of IoT and IIoT markets. Following the joining of forces between the IIC and OFC, the IIC will expand its effort to clarify distributed computing at and near the cyberphysical boundary of IIoT systems and continue to provide an ecosystem for the advancement of the IIoT.

5.1 IIC PLANS

The IIC continues to provide clarity and guidance to the market around IIoT systems. There are multiple initiatives to provide further detail around IIoT security and distributed computing in edge environments. The IIC recently released Managing and Assessing Trustworthiness for IIoT in Practice,[17] the IoT Security Maturity Model[18] and a Practitioner's Guide for that Security Maturity Model.[19] Additional security guidance and frameworks are forthcoming as well as a Trustworthiness Framework. The IIC also released a white paper on edge computing and combined with the OFC to more fully address the promise of edge computing.

The IIC continues to support multiple member teams in their testbed projects and will expand its initiatives with industry consortia, standards organizations and other liaisons. The integration of several testbeds from the OFC drives an expanded portfolio of testbeds addressing this critical area of edge computing with further resources from academia and Asia-Pacific members.

As for liaisons, this joint white paper is an example of liaison initiatives to provide additional market clarity. With this joint paper with oneM2M, the IIC is providing additional market clarity and expects this joint work to continue with additional integration and guidance.

To organize and simplify access to the various documents and results of the IIC's work, the IIC Resource Hub[20] is a new interface to IIoT industry knowledge and expertise. This knowledge and expertise are represented in IIC documents, testbed insights, toolkits, demos and relationships with standards and industry groups around the world. The IIC expanded this new interface to the library of knowledge by providing web-based tools guiding user through the analysis and planning of their own IIoT project and maturity assessment, referencing IIC resources and providing actionable intelligence.

---

[17] https://www.iiconsortium.org/pdf/Managing_and_Assessing_Trustworthiness_for_IIoT_in_Practice_Whitepaper_2019_07_29.pdf

[18] https://www.iiconsortium.org/pdf/SMM_Description_and_Intended_Use_2018-04-09.pdf

[19] https://www.iiconsortium.org/smm.htm

[20] https://www.iiconsortium.org/resource-hub.htm

IIC's various technical groups are working on a set of technical reports, whitepapers and best practices to further enrich its technical offerings to the IIoT community, including *Industrial Internet Networking Framework, Digital Twin Interoperability, Implementing Edge Computing, Trustworthiness Framework, Software Trustworthiness in Digital Twins, Communications and Connectivity Security Best Practices, Industrial Artificial Intelligence, Characteristics of IIoT Information Models, Implementation Aspect: IIoT and Blockchain and Industrial Distributed Ledger*, etc.

5.2 oneM2M Plans

oneM2M functions as an iterative standardization body, releasing successive updates to its technical specifications to incorporate new requirements. Release 1 of the standard, issued in 2015, defined a minimum deployable horizontal common service layer. In 2016, oneM2M delivered Release 2 of the technical specification. This enabled interworking capabilities with other IoT proximal network technologies, an enhanced security framework and services for describing and discovering devices and data based on semantic descriptions. Towards the end of 2018, oneM2M issued its Release 3 technical specifications. Some of its key features includes integration capabilities between oneM2M and 3GPP standards to deliver service quality capabilities at mobile-industry scale. As detailed below, members of oneM2M's Technical Plenary are working on Release 4 of the standard and incorporating feedback from Release 3 implementation and testing activities.

Currently, work is underway on Release 4 to address edge computing, 3GPP interworking, vehicular applications and semantic interoperability amongst other topics.

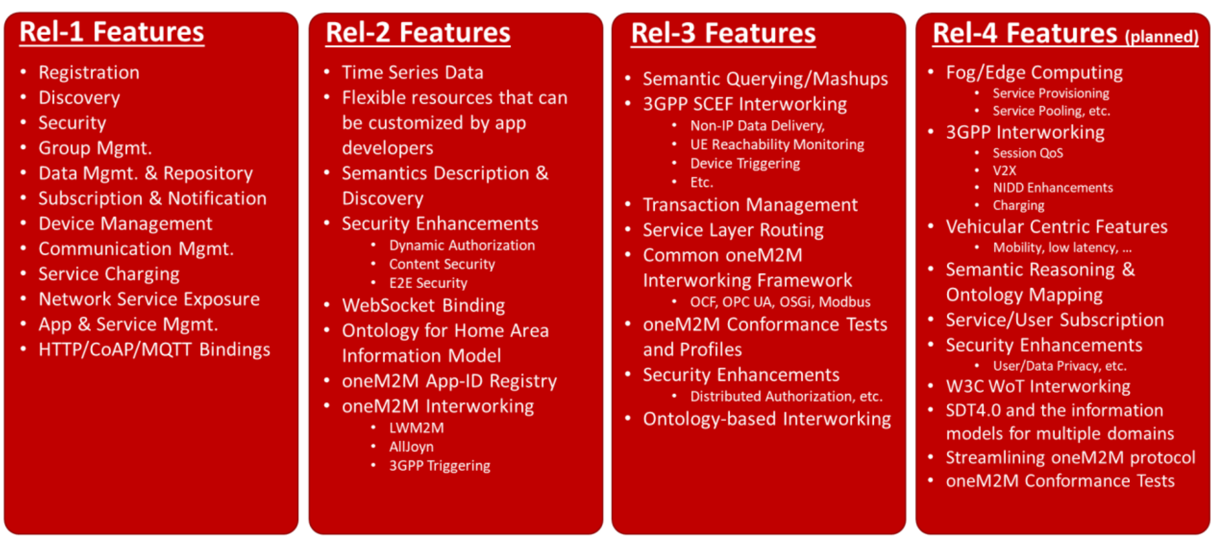

Figure 12 oneM2M Feature Summary by Release (Source: oneM2M)

In parallel with its standardization efforts, oneM2M inaugurated a certification process to facilitate market adoption.

5.3 Conclusions and Next Steps

Following an introductory workshop, a sub-group formed of IIC and oneM2M members agreed to share information about their respective organizations across the member base and the wider IoT community. This lays the groundwork for future collaboration as both organizations share a common purpose to foster the market for IIoT solutions.

With a focus on practical deployment tools, this document describes and compares the IIC's and oneM2M's architectural approaches. This analysis highlights strong alignment, favoring implementation methodologies, reusable components and scalable solutions. These are supported by a toolkit of best practices and technical standards for organizations involved in the design and deployment of IIoT systems.

The process of exchanging information and furthering the IIC-oneM2M liaison has deepened knowledge across the two institutions and identified common areas for future collaboration. The priority topics for joint exploration and evaluation include the following areas:

- IoT security approaches and solutions,
- enablers of semantic interoperability, including potential frameworks for cross-domain data models,
- new requirements emerging from industrial IoT use-cases,
- edge, fog and distributed computing approaches and solutions and
- networking and connectivity solutions and best practices.

6 Legal Notices