ETSI TR 118 518 V2.0.0 (2016-09)

oneM2M;
Industrial Domain Enablement
(oneM2M TR-0018 version 2.0.0 Release 2)

Reference
DTR/oneM2M-000018

Keywords
IoT, M2M

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Important notice

The present document can be downloaded from:
http://www.etsi.org/standards-search

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the only prevailing document is the print of the Portable Document Format (PDF) version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status.
Information on the current status of this and other ETSI documents is available at
https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx

If you find errors in the present document, please send your comment to one of the following services:
https://portal.etsi.org/People/CommiteeSupportStaff.aspx

Copyright Notification

Contents

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (https://ipr.etsi.org/).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

This Technical Report (TR) has been produced by ETSI Partnership Project oneM2M (oneM2M).

1 Scope

The present document collects the use cases of the industrial domain and the requirements needed to support the use cases collectively. In addition it identifies the necessary technical work needed to be addressed while enhancing future oneM2M specifications.

2 References

2.1 Normative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

Referenced documents which are not found to be publicly available in the expected location might be found at https://docbox.etsi.org/Reference/.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

The following referenced documents are necessary for the application of the present document.

Not applicable.

2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] oneM2M Drafting Rules.

NOTE: Available at http://www.onem2m.org/images/files/oneM2M-Drafting-Rules.pdf.

[i.2] ETSI TS 118 111: "oneM2M; Common Terminology (oneM2M TS-0011)".

[i.3] IEC TC News, http://www.iec.ch/tcnews/2014/tcnews_0214.htm.

[i.4] http://www.is-inotek.or.jp/archive/05_Ishikuma_Smart_Manufacturing.pdf, Dec 2014.

[i.5] IIC website, http://www.industrialinternetconsortium.org/.

[i.6] IIC document 'Engineering: The First Steps', Sep 2014.

[i.7] IIC report 'Engineering Update: November 2014', Nov 2014.

[i.8] IEEE P2413 website, http://grouper.ieee.org/groups/2413/.

[i.9] IEEE P2413 presentation 'Standard for an Architectural Framework for the Internet of Things (IoT)', Sep 2014.

[i.10] IEEE P2413 report 'oneM2M Specification Comment Collection', Oct 2014.

[i.11] SMLC website, https://smartmanufacturingcoalition.org/.

[i.12] SMLC presentation, March 2014.

NOTE: Available at https://smartmanufacturingcoalition.org/sites/default/files/savannah_rivers_03-10-2014.pdf.

[i.13] Article "First European testbed for the Industrial Internet Consortium" in Bosch's ConnectedWorld Blog http://blog.bosch-si.com/categories/manufacturing/2015/02/first-european-testbed-for-the-industrial-internet-consortium/.

[i.14] ETSI TS 118 102: "oneM2M; Requirements (oneM2M TS-0002)".

[i.15] ETSI TS 118 101: "oneM2M; Functional Architecture (oneM2M TS-0001)".

[i.16] IEC 62443 series: "Industrial communication networks - Network and system security".

[i.17] ETSI TS 118 103: " oneM2M; Security Solutions (oneM2M TS-0003)".

[i.18] NIST Special Publications (SP)800-57: "Guidelines for Derived Personal Identity Verification (PIV) Credentials".

[i.19] Draft Recommendation ITU-T X.iotsec-1: "Simple encryption procedure for Internet of Things (IoT) environments".

[i.20] ETSI TR 118 518: "oneM2M; Industrial Domain Enablement (oneM2M TR-0018)".

[i.21] IEC TC 65: "Industrial-process measurement, control and automation".

[i.22] Reference Architecture Model Industrie 4.0 (RAMI4.0), July 2015.

NOTE: Available at https://www.vdi.de/fileadmin/vdi_de/redakteur_dateien/gma_dateien/5305_Publikation_GMA_Status_Report_ZVEI_Reference_Architecture_Model.pdf

3 Abbreviations

For the purposes of the present document, the terms and definitions given in ETSI TS 118 111 [i.2] and the following apply. A term defined in the present document takes precedence over the definition of the same term, if any, in [i.2].

ACP	Access Control Policy
AES	Advanced Encryption Standard
CR	Change Request
CSE	Common Services Entity
DCS	Distributed Control Systems
DMZ	Demilitarized Zones
DoS	Denial of Service
DSL	Digital Subscriber Line
DTLS	Datagram Transport Layer Security
FIPS	Federal Information Processing StandardizationGPS Global Positioning System
GSM	Global System for Mobile Communication
IACS	Industrial Automation & Control System
ID	Identifier
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronic Engineers
IIC	Industrial Internet Consortium
IN	Infrastructure NodeIPE Interworking Proxy application Entity
ISDN	Integrated Services Digital Network
ITU-T	International Telecommunication Union Telecommunication Standardization Sector
LAN	Local Area Network
MIC	Message Integrity Code
MN	Middle Node
NSE	Network Service EntityPLCProgrammable Logic Controllers
QoI	Quality of Information
QoS	Quality of Service
RBAC	Role-based Access Control

SHA	Secure Hash Algorithm
SL	Security Level
SMB	Standardization Management Board
SMLC	Smart Manufacturing Leadership Coalition
SOA	Service Oriented Architecture
TLS	Transport Layer Security
UMTS	Universal Mobile Telecommunications System
VPN	Virtual Private Network
WiFi	Wireless Fidelity
WLAN	Wireless Local Area Network
XML	eXtensible Markup Language

4 Conventions

The key words "Shall", "Shall not", "May", "Need not", "Should", "Should not" in the present document are to be interpreted as described in the oneM2M Drafting Rules [i.1].

5 Introduction to Industrial Domain

5.1 Industrial Domain Overview

In previous industrial domains, the information exchange from factory-to-factory or centre-to-factory needed support from humans. Normally the exchange is non-synchronous, discrete, inefficient and unable to achieve the capacity to respond rapidly to market changes.

Currently M2M technologies are considered to achieve the communication and interaction from machine-to-machine without human support. It brings opportunities to achieve synchronous, continuous and effective information exchange in manufacturing scenarios. Based on M2M, new manufacturing methods can be suitable to increase complex requirements of future market needs.

Many industrial companies are aware of the potential power to update traditional manufacturing systems by introducing M2M technologies. They are not restricted to the technical requirements, such as improving the performance of productivity, quality, delivery, cost reduction and security, but also new opportunities to cooperate with other domains for mass production, and the potential to build the new architecture for next generation industry. Figure 5-1-1 is an example architecture.

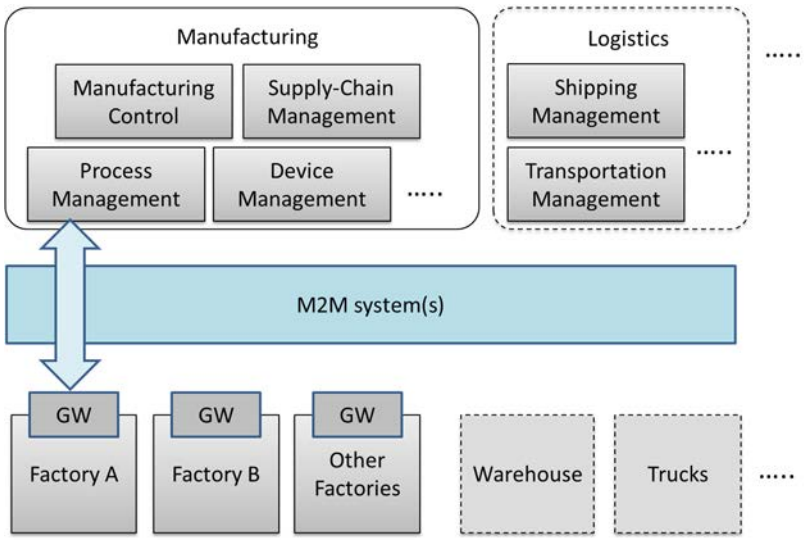

Figure 5-1-1: Industrial Domain Architecture

In figure 5-1-1, factories will be connected with manufacturing services via the M2M system(s). Generally, the gateway in the factory will collect data from the factory and send it to manufacturing services in a management centre. The service will be initiated by different management modules and sent to factories.

In addition, with the M2M system(s), the complex service can be sent to several factories synchronously, to enable effective collaboration between factories. Every factory is expected be able to make accurate decisions and to operate effectively, because it can work based on the results of data analysis and the data is from all the factories rather than from only one. The management centre with manufacturing services is also expected to be able to make accurate decisions by utilizing field data from all factories, and also via other support systems, such as cloud computing, to improve efficiency of local or global services.

In the future, if more and more industry related domains, such as logistics and power management systems, can be connected into the M2M system, resources (warehouses, trucks, ships, power, etc.) can be integrated efficiently. Therefore more flexible services will be created to face this complex situation.

As the oneM2M architecture provides general Application Layer, Common Services Layer and the Underlying Network Services Layer, and will be connected with other vertical systems, it is important to consider the integration of industrial domain systems with the oneM2M architecture.

5.2 Technology Trends in Industrial Domain

To accelerate the update of manufacturing systems, many worldwide organizations have been established and have started making efforts.

In June 2014, the IEC (International Electrotechnical Commission), Standardization Management Board (SMB) set up a Strategy Group, SG8, to deal with a number of tasks related to Smart Manufacturing [i.3].

Table 5.2-1: Industrial Domain Research in IEC SMB SG8 [i.4]

Mission & Scope	• Develop a function model/reference architecture that helps to identify gaps in standardization based on to-be-collected use cases. • Develop a common strategy for the implementation of Industry 4.0. • Extend standards towards: environmental conditions, security, properties, energy efficiency, product and functional safety.
Technical Keywords	• Industrial process measurement, control and automation. • Application: semantics relationships descriptive technologies. • Services: web services /SOA repositories /cloud dependable connections. • Communication: data access real-time communications.

The IIC (Industrial Internet Consortium) was founded in March 2014 to bring together the organizations and technologies necessary to accelerate growth of the Industrial Internet by identifying, assembling and promoting best practices [i.5].

Table 5.2-2: Industrial Domain Research in IIC [i.6] and [i.7]

Mission & Scope	• Productivity and efficiencies can be improved by production process governing themselves with intelligent machines and devices. • Real time data report from handheld digital device. • Wearable sensors track location of employees in case of emergency. • Future scenarios: new steering instruments will interlink things to ensure the entire value chain and trigger adjustments on the factory floor in case of chain changing; raw materials will be programmed to record standard process and their customer to realize automatic customization.
Technical Keywords	• Representative use case areas include connectivity, logistics, transportation, and healthcare. • Key capabilities system characteristics including resilience, safety and security. (such as key system characteristic, intelligent and resilient control, operations support, connectivity, integration and orchestration, security, trust and privacy, and business viewpoint). • Data management and analytics. • Security: endpoint security, secure communications and security management and monitoring (currently focused on general security use case).

IEEE P2413 defines an architectural framework for the Internet of Things (IoT), which includes descriptions of various IoT domains including the industrial domain and is sponsored by the IEEE-SA [i.8].

Table 5.2-3: Industrial Domain Research in IEEE P2413 [i.9] and [i.10]

Mission & Scope	• Ranges from the connected consumer to smart home & buildings, e-health, smart grids, next generation manufacturing and smart cities. • Promote cross-domain interaction instead of being confined to specific domains.
Technical Keywords	• Energy efficiency during data transmission. • Areas of interest: industrial Internet, cross sector common areas, common architecture, security safety privacy.

The SMLC (Smart Manufacturing Leadership Coalition) is a non-profit organization committed to the development and deployment of Smart Manufacturing Systems. SMLC activities are built around industry-driven development, application and scaling of a shared infrastructure that will achieve economic-wide impact and manufacturing innovation [i.11].

Table 5.2-4: Industrial Domain Research in SMLC [i.12]

Mission & Scope	• To build a cloud-based, open-architecture platform that integrates existing and future plant level data, simulations and systems across manufacturing seams and orchestrate business real time action.
Technical Keywords	• Cloud-based networked data. • Enterprise real-time. • Plant level data. • Information & action. • Security.

Plattform Industrie 4.0 is the central alliance for the coordination of the digital structural transition in German industry and unites all of the stakeholders from business, associations, trade unions and academia. Results so far have been summarized under the title “Reference Architecture Model Industrie 4.0 (RAMI4.0)”. RAMI 4.0 provides a conceptual superstructure for organizational aspects of Industrie 4.0, with emphasis on collaboration infrastructures and on communication structures. It also introduces a concept of an administration shell that covers detailed questions on semantic standards, technical integration and security challenges. RAMI4.0 will be published as DIN SPEC 91345 " Reference Architecture Model Industrie 4.0” (RAMI4.0).

Table 5.2-5: Industrial Domain Research in Plattform Industrie 4.0 [i.22]

Mission & Scope	• Identify all relevant trends and developments in the manufacturing sector and combine them to produce a common overall understanding of Industrie 4.0 • Develop ambitious but achievable joint recommendations for all stakeholders, that serve as the basis for a consistent and reliable framework • Identify where action is required on standards and norms and actively express recommendations for national and international committee work
Technical Keywords	• Reference architectures, standards and norms • Incorporate existing norms and standards in RAMI4.0 (Reference Architecture Model Industrie 4.0). RAMI4.0 is an initial proposal for a solution-neutral reference architecture model. • Research and innovation • Evaluate current case studies to identify research and innovation requirements from the industry perspective. • Security of networked systems • Resolve the outstanding issues concerning secure communication and secure identities of value chain partners. • Detect cyber attacks on production processes and their implications.

Based on the information above and the current oneM2M architecture, the technology trends below are becoming more and more important:

- Data management and analytics:

In some industrial organizations, data management and data analytics are independent layers for data processing (such as filtering and catalogue management) and data analytics. Since large amounts of data are generated in industrial scenarios, further functionality design for data management and data analytics CSFs may need to be considered in oneM2M.

- Real-time command and control:

M2M technologies enable real-time response manufacturing practices in complex supplier networks. Realizing real-time command and control by highly available and time critical technologies will bring benefits to process automation and the optimization of supply chains. Use cases with real-time command and control features may need to be considered in oneM2M. Additionally, requirements from these use cases may need to be taken into consideration.

- Connectivity:

Since connectivity in the industrial domain needs to co-exist and evolve with legacy protocols, legacy connectivity (both wired and wireless) and legacy wiring, connectivity for manufacturing processes needs to be considered and this may have an impact on NSE functionalities.

- Security:

Increased networking and wireless technologies are the main security concerns for industrial companies. Undoubtedly, the risk trade-off will not stop companies from manufacturing evolution. Thus a renewed risk for management and ensuring security for the industrial domain may need to be considered.

Meanwhile more trends, such as web services over M2M devices and protocols in industrial domain, will be further tracked and analyzed.

6 Use Cases

6.1 An Industrial Use Case for On-demand Data Collection for Factories

6.1.1 Description

In factories, a lot of data are created from Programmable Logic Controllers (PLCs) every second, and data are utilized to monitor production lines. This data is available via industrial bus systems, e.g. Real-time Ethernet. In order to monitor remotely, data is gathered by the M2M service platform that needs to interface with such industrial bus systems via M2M gateways. However, it is difficult to gather all data to the M2M service platform because sometimes more than 1mega bit data is created per second. In such cases, only necessary data is gathered depending on situations and filtering / pre-processing of the raw data needs to be performed at the gateways.

This use case proposes that the oneM2M System offers pre-processing capabilities, e.g. rule-based collection policies (averages, thresholds, etc. …). These rules (e.g. in XML format) are called “"data catalogues”".

6.1.2 Source

- REQ-2014-0487R03: A use case for industry: On-demand data collection for factories.
- REQ-2015-0551: CR to ETSI TR 118 518 [i.20] Use Case 6.1.