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.

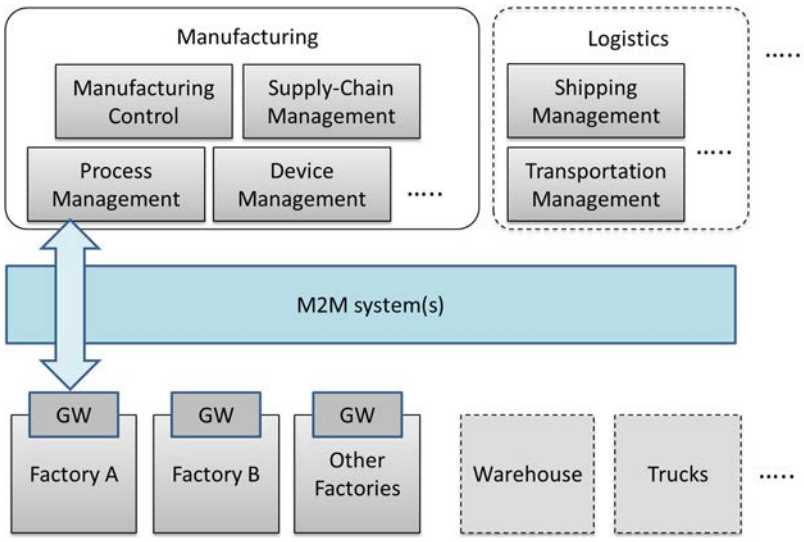


Figure 5-1-1: Industrial Domain Architecture

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.

6.1.3 Actors

- PLC: It controls sensors and devices in a production line according to embedded programs. It also has interface to Real-time Ethernet. It broadcasts data related to the production line to Real-time Ethernet.
- M2M Gateway: It provides an interface from the Real-time Ethernet to the oneM2M System. An application on the gateway collects necessary data from Real-time Ethernet according to the configuration called data catalogue, and send collected/pre-processed data to M2M service platform.
- M2M service platform: It stores data gathered from gateway(s), and provide data to applications. It also manages data catalogue in gateway(s).
- Application: An M2M Application in the Infrastructure Domain that monitors production lines by using collected data in M2M service platform, and send change request of data catalogue depending on situations.
- Real-time Ethernet: A technology standardized in IEC TC 65 [i.21]. Ethernet is used at the physical layer, but upper protocol is designed for industry purpose. In this use case, broadcast protocol is assumed. On top of Ethernet cable, data is broadcast with ID. Address configuration is not necessary here.
- Internet connection: M2M service platform and gateway(s) are connected by the Internet physically.

6.1.4 Pre-conditions

- PLCs and the gateway are connected to the Real-time Ethernet. PLCs broadcast data to the Real-time Ethernet. The Gateway is configured to pick up necessary data from the Real-time Ethernet.
- On top of the internet, a VPN connection is established between the M2M service platform and the gateway(s).
- The data catalogue is managed by the M2M service platform.

6.1.5 Triggers

- Data catalogue is configured for the gateway to pick up data in the Real-time Ethernet.

6.1.6 Normal Flow

- The Gateway picks up the broadcasted data. It picks up only data that matches conditions described in the data catalogue. If data does not match the conditions, the gateway ignores the data.
- The Gateway sends the collected data to the M2M service platform.
- The M2M service platform receives the data and stores it.
- The application utilizes the data. For example, it monitors the status of the production line.
- If the application user finds some problems in a production line, he/she changes the data catalogue in the M2M service platform to collect all data related to the production line and sends the data catalogue to the targeted gateway.

6.1.7 High Level Illustration

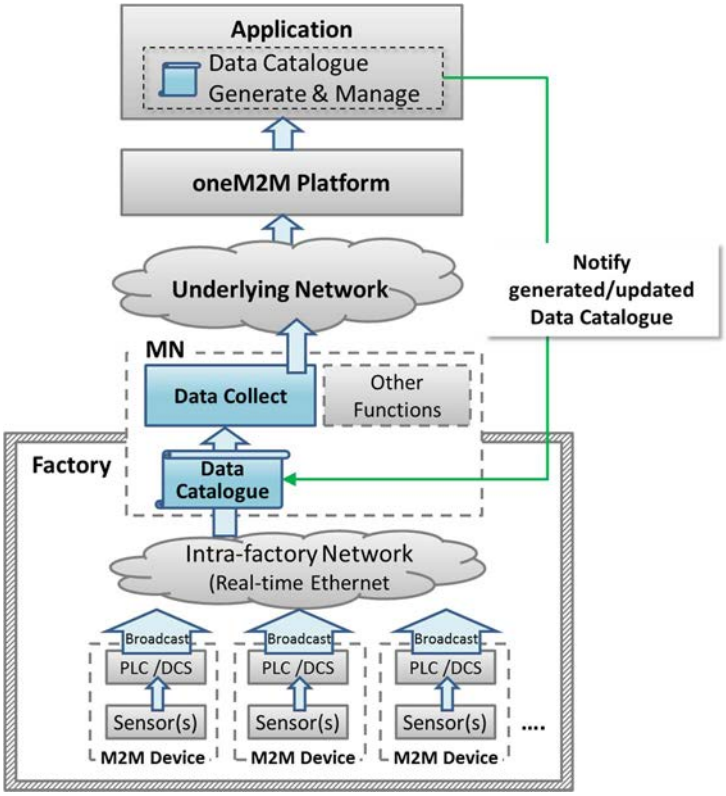


Figure 6.1.7-1: High-level Illustration of On-demand Data Collection for Factories

6.1.8 Potential Requirements

1) The gateway shall be able to collect data from the field area network (e.g. industrial bus systems) according to the data collection policy stored in the gateway.

2) The data collection policy shall be manageable (configured, updated, deleted, etc.) by M2M Applications on the M2M service platform.

6.2 Integrity of Data Collection Monitoring

6.2.1 Description

In factories, a lot of data is created from PLCs every second and data is utilized to monitor production lines. This data is available via industrial bus systems, e.g. Real-time Ethernet.

This type of data is called time series data which is a sequence of data points, typically consisting of successive measurements made over a time interval.

In order to monitor remotely, data is gathered by the oneM2M service platform that needs to interface with such industrial bus systems via the M2M gateway (MN).

When some of the data is lost due to various reasons, such as, damage of production line, temporal network delay, continuous network capacity overload and so on, action will be required immediately for safety reasons. In addition, some considerations may be necessary, such as switching to a new network service with larger capacity, changing to the backup network or adjusting data collecting policy to address the original cause of data loss. Other considerations may be effective when remote monitoring application queries the oneM2M platform about the condition of network traffic, e.g. temporal delay, continuous capacity overflow, or connection failure.

Similar to the remote monitoring application, the MN in each factory receives the results of analysis or some commands, which could be lost due to for example, failure in analysis process, temporal network delay, or continuous network capacity overflow. The MN can detect the loss when the analysis results or the commands are in the form of time series data, or it can detect potential loss by monitoring the condition of network traffic. When temporal network delay or continuous network capacity overflow occurs, analysis results or commands may be lost. This loss also requires immediate decision and addressing at the root cause.

This use case proposes that the oneM2M System shall be able to provide the capability to collect, store time series data as well as monitor the integrity of the data.

Additionally, the oneM2M System shall be able to provide the capability to monitor the condition of network traffic.

6.2.2 Source

- REQ-2015-0522R04: Integrity of Data Collection Monitoring.

6.2.3 Actors

- PLC: It controls sensors and devices in a production line according to embedded programs. It also has interface to Real-time Ethernet. It broadcasts data related to the production line to Real-time Ethernet.
- MN: It provides an interface from the Real-time Ethernet to the oneM2M System. The gateway collects and stores time series data from Real-time Ethernet then sends them to the oneM2M service platform. It also receives analysis results or commands from the oneM2M service platform. Furthermore, the gateway monitors the integrity of received analysis results or commands by monitoring the condition of the network. It can detect a loss when the analysis results or the commands are in the form of time series data, or it can detect potential loss with the help of monitoring the condition of the network traffic when temporal network delay or continuous network capacity overflow occurs.
- oneM2M service platform: It stores data gathered from gateway(s), and provides data to applications.
- Application: An M2M Application in the Infrastructure Domain monitors production lines by using collected data in the oneM2M service platform and sends analysis results or commands depending on the situation.
- Real-time Ethernet: A technology standardized in IEC TC 65 [i.21]. Ethernet is used at the physical layer, however the upper protocol is designed for industry purposes. In this use case, broadcast protocol is assumed.
- Internet connection: the oneM2M service platform and gateway(s) are connected by the Internet physically.

6.2.4 Pre-conditions

- PLCs and the gateway are connected to the Real-time Ethernet. PLCs broadcast data to the Real-time Ethernet. The Gateway is configured to pick up necessary data from the Real-time Ethernet.
- On top of the internet, a VPN connection is established between the oneM2M service platform and gateway(s).

6.2.5 Triggers

- The gateway starts to receive time series data.

6.2.6 Normal Flow

The Gateway picks up time series data which is broadcasted via Real-time Ethernet. The gateway sends collected data to oneM2M service platform.

oneM2M service platform receives data, then stores it and sends it to the application.

The application monitors the integrity of the time series data which is sent from the gateway. If data loss occurs, the application user will send a command for immediate control action. Then the application user will check the condition of the network traffic to determine which means are used to solve the data loss.

6.2.7 High Level Illustration

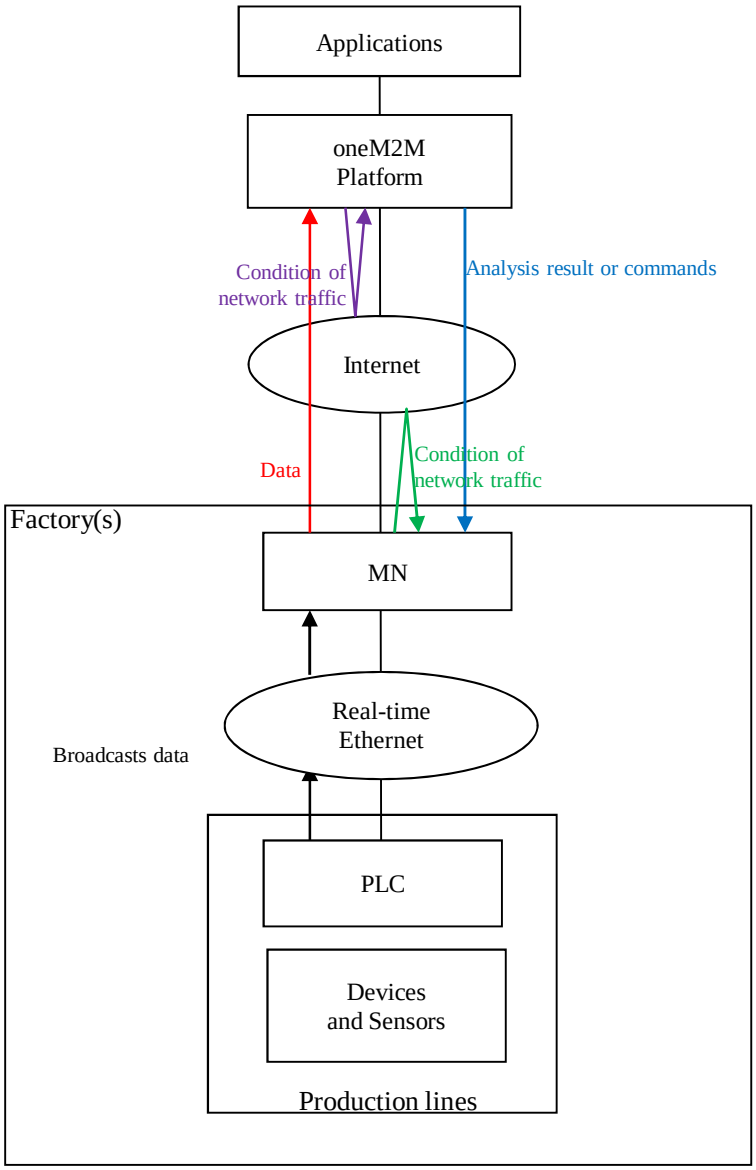


Figure 6.2.7-1: High-level Illustration of Integrity of Data Collection Monitoring

6.2.8 Potential Requirements

1) The oneM2M System shall be able to collect and store time series data, as well as monitor the integrity of this data.

2) The oneM2M System shall be able to provide the capability to monitor the condition of the network traffic.

6.3 Data Process for Inter-factory Manufacturing

6.3.1 Description

To achieve remote manufacturing, numerous sensors are placed at production lines in factories and a significant amount of data is generated for monitoring purposes. This data is broadcast via an intra-factory network (e.g. real-time Ethernet) through PLCs or Distributed control Systems (DCS), etc. For monitoring product lines efficiently and effectively, Middle Nodes (MNs) (which means the gateway) will selectively collect necessary data from an intra-factory network and then send this data to the oneM2M services platform for use by manufacturing control applications. The data collection policy (named data catalogue) utilized at the MNs is generated and managed by the application layer and may vary based on the specific monitoring purpose (e.g. collect only temperature data for the purpose of monitoring device temperature, or collect both humidity and gas data in order to monitor product quality).Data process functionality is also needed at the MNs in order to filter out error data or to summarize the percentage of data exceeding a threshold.

To respond rapidly to market changes, new factories may be needed to ensure sufficient productivity. Thus inter-factory collaboration provides significant benefit and efficiency which can be used in establishing a new factory where the reference data catalogue can be used to establish a new environment.

6.3.2 Source

- REQ-2015-0552R01: Data Process for Inter-factory manufacturing.

6.3.3 Actors

M2M Device: Sensors, controllers etc. located in factories (e.g. located at product lines) which measure and generate data. The PLC /DCS control sensors in production lines according to embedded programs. Both PLC and DCS can broadcast data related to production lines to intra-factory networks.

Intra-factory Network: In this use case, real-time Ethernet is assumed. It is standardized in IEC TC 65 [i.21] for which Ethernet is used at physical layer, but upper protocol is designed for industrial purposes. Meanwhile, broadcast protocol is assumed and data is broadcast with unique identifier/parameter (e.g. device ID).

oneM2M MN: The MN provides an interface from the intra-factory network to the oneM2M System. The MN collects data from the intra-factory network according to the data catalogue, which is the data collection policy. The MN may process collected data and send the data to the oneM2M services platform through the underlying network.

oneM2M Services Platform: The oneM2M services platform stores data gathered from MNs, and provides data to applications.

oneM2M Application: A oneM2M application in the Infrastructure Domain that monitors production lines for remote manufacturing control by using collected data from the oneM2M services platform. For monitoring purposes, the M2M application defines and generates the data catalogue, then, the application provides the data catalogue to MNs. The M2M application also shares data catalogue in the MNs with other factories.

6.3.4 Pre-conditions

The PLCs or DCSs control sensors in production lines according to embedded programs. Both PLC and DCS can broadcast data related to production lines into an intra-factory network.

Real-time Ethernet is assumed as the intra-factory network. Broadcast protocol is assumed and real-time Ethernet data is broadcast with a unique identifier/parameter (e.g. device ID).

6.3.5 Triggers

A remote manufacturing control application generates a data catalogue to collect data from product lines in factories.

6.3.6 Normal Flow

The normal flow steps are as follows:

1) The application generates the data collection policy into a data catalogue, or updates the data catalogue when the monitoring purpose has changed. The application then notifies the data catalogue to the MNs in a factory.

2) The application providing the data catalogue to the MNs may include the following condition:

   - In some inter-factory collaboration cases, the application also provides the data catalogue to the MNs in other collaborating factories, e.g. a newly built factory.

3) MNs start to selectively collect data from real-time Ethernet according to the data catalogue.

4) The oneM2M services platform receives, stores and provides the data to manufacturing control applications.

5) The application analyses collected data for remote manufacturing control.

6.3.7 Post-conditions

The application utilizes (e.g. monitors and analyses) the data collected according to the data catalogue.

6.3.8 High Level Illustration

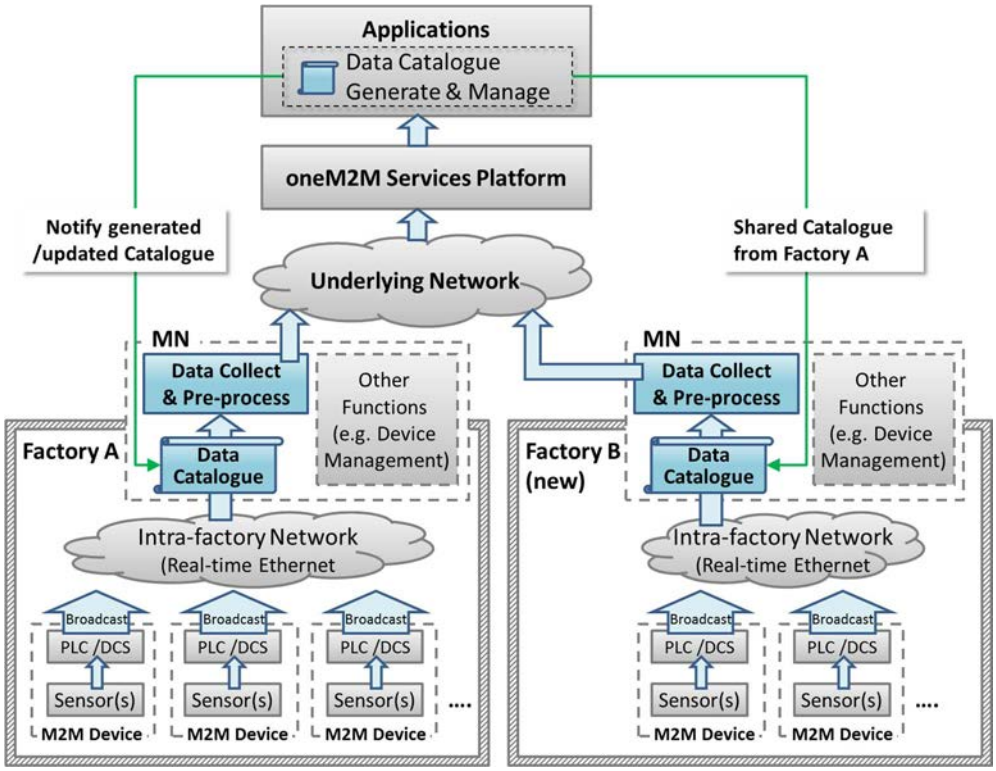


Figure 6.3.8-1: High-level Illustration of Data Process for Inter-factory Manufacturing

6.3.9 Potential Requirements

1) The oneM2M system shall be able to share data collection policies among different applications.

6.4 Aircraft Construction and Maintenance

6.4.1 Description

In aircraft construction, there are precise regulations that specify the type of screw and the amount of force that needs to be used to join specific parts. When it comes to passenger aircraft, there are thousands of such screws that have to be tightened and precisely documented. Joints on the wings naturally require a different amount of force than those on an aircraft window.

The tools are Wi-Fi-enabled and can identify their precise location on the shop floor. The position of the aircraft in the hangar is also fixed. With fixed coordinates and Wi-Fi connectivity, we know, for example, that a particular tool is located at the vertical stabilizer. Instructions that specify the force it should use to tighten screws can automatically be sent to the tool.

Although this use case focuses on aircraft construction and maintenance, the connected power tool technology is expected to be effective in more applications:

- Safety-critical work processes are closely monitored and analysed. Anomalies are automatically detected through the central processing, analysis, and visualization of production process data in near real time. Role-specific alerts can be triggered automatically.
- The power tool fleet manager has an exact overview of the power tool fleet status and utilization thanks to central access to process data. Organizational processes can be triggered automatically.
- Quality controls are automated and shifted to earlier stages of the production process. For example, hundreds of thousands of torque recordings are made available in their entirety for quality monitoring.
- Indoor geofencing alarms ensure that power tools are used according to regulations. Not all tools are allowed for all production and maintenance steps, e.g. in aircraft maintenance. As soon as power tools know their location, they can switch off when used in error.

6.4.2 Source

- REQ-2015-0562R01: Aircraft Construction and Maintenance.

NOTE: This use case refers to an article "First European testbed for the Industrial Internet Consortium" in Bosch's ConnectedWorld Blog [i.13].

6.4.3 Actors

- Power tools: People in a shop floor utilize them to tighten screws of the airplane. They are Wi-Fi-enabled, and can identify their precise location on the shop floor. They receive instruction for the amount of power needed to tighten screws.
- Indoor localization technology: The technology is utilized to identify the location of the power tools.
- oneM2M service platform: the oneM2M service platform receives location information for the power tools and sends it to the application. It also receives instructions for the amount of power needed to tighten the screws and sends it to each one of the power tools.
- Application: In this use case, the application is for aircraft construction and maintenance. It holds the position of the aircraft in the hangar and matches it to the location information of the power tools to calculate which power tool is utilized for which part of the aircraft. Then it gets instructions that specify the force a power tool should use to tighten screws by utilizing regulations that specify the kind of screw and the amount of force that has to be used to join specific parts. Finally, it sends the instructions to each one of the power tools.
- Underline network: In this use case, Wi-Fi is assumed.

6.4.4 Pre-conditions

- The application holds the position of the aircraft in the hanger and the regulations that specify the kind of screw and the amount of force that has to be used to join specific parts.
- Power tools are Wi-Fi-enabled.

6.4.5 Triggers

- A person on a shop floor starts to use a power tool.

6.4.6 Normal Flow

1) The power tool identifies precise location information with the use of indoor localization technology and sends the information to the oneM2M platform.
2) The oneM2M service platform receives the location information and sends it to the application.
3) The application matches the position of the aircraft in the hanger to the location information of the power tool to calculate for which part of the aircraft the power tool is used.
4) The application gets instructions that specify the force the power tool should use to tighten screws by utilizing regulations that specify the kind of screw and the amount of force that needs to be used to join specific parts.
5) The application sends the instruction to the oneM2M platform.
6) The oneM2M platform receives the instruction and sends it to the power tool.
7) The power tool uses the specified amount of force to tighten a screw.

6.4.7 High Level Illustration

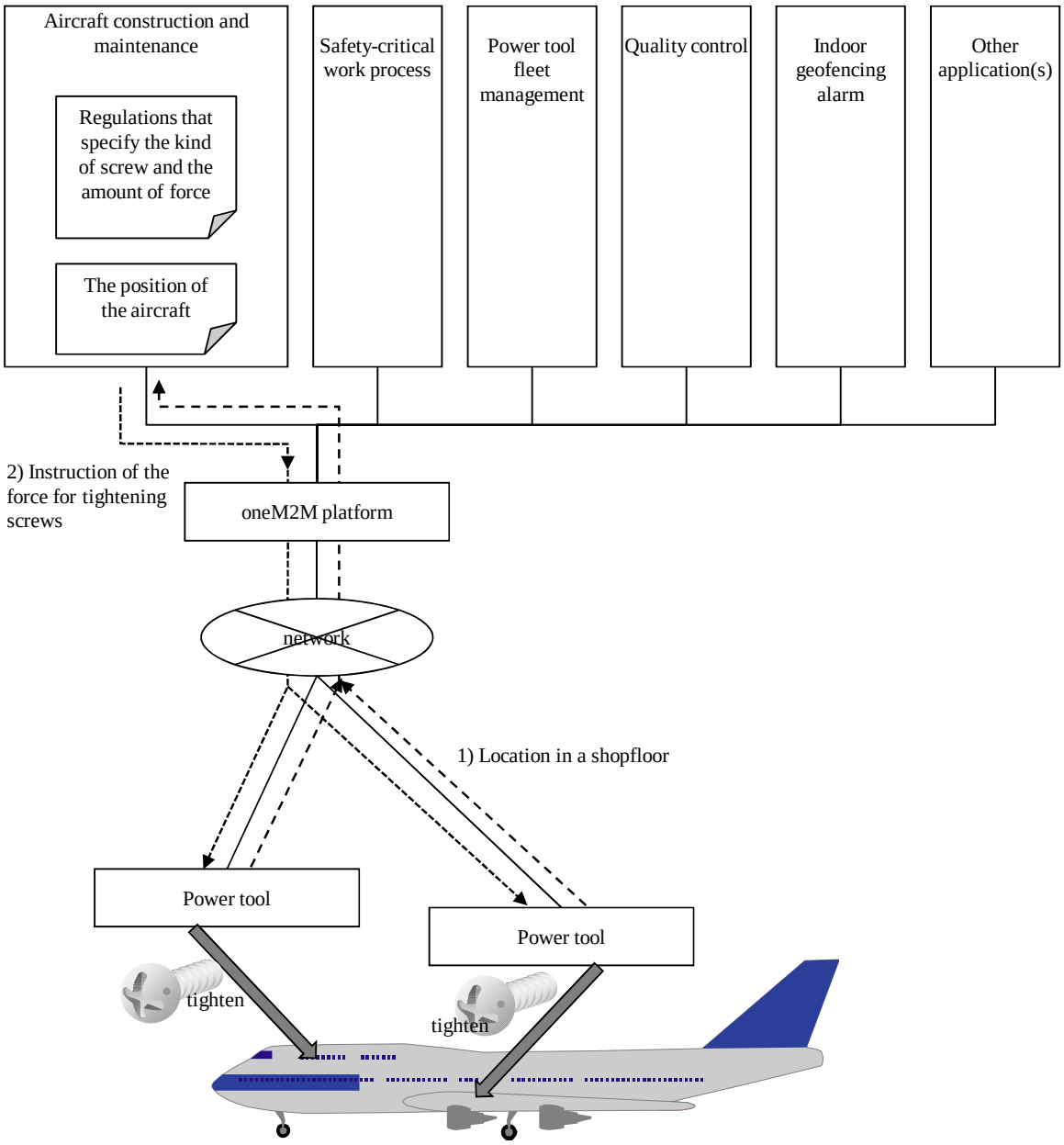


Figure 6.4.7-1: High-level Illustration of Aircraft Construction and Maintenance

6.4.8 Potential Requirements

1) The oneM2M System shall be able to support mechanisms for the M2M Devices and/or Gateways to report their geographical location information to M2M Applications (OSR-047 [i.14]).

2) The oneM2M System shall support the ability for single or multiple M2M Applications to interact with a single or multiple M2M Devices/Gateways (application in the device/gateway) (OSR-009 [i.14]).

6.5 Real Time Data Collection

6.5.1 Description

In automated production using information and communication technology, behaviours of devices are controlled according to sensor values. In order to achieve adequate control, real-time Ethernet, with which sensors and devices are connected through controllers, are required to provide real-time transmission and a high level of reliability. Real-time Ethernet is standardized in IEC TC 65 [i.21] and has characteristics such as the following:

- It enables real-time transmission by message priority control, according to the importance of the data (network re-configuration communication is first, time series data is second, controlling commands for devices are third, and information data is the forth priority). "Information data" contains video, audio data or objected sensor data. Higher priority data can be transmitted without interference from lower priority data. Priority of data depends not only on the kind of data but also on source node or destination node. For example, although controlling commands for devices shall not be delayed, log information for logging servers does not require strict real-time transmission. Therefore the data have a different value of priority.

- When real-time Ethernet is introduced, size and frequency of high priority data transmission are designed to ensure that the total volume of sent data does not exceed the capacity. With this design, real-time transmission is ensured and time series data and controlling commands are received within pre-defined intervals.

- It utilizes a duplex LAN, which consists of two physically independent network paths between end-nodes, or dual Node to provide a high level of reliability.

- It achieves a high level of reliability on the basis of operations on ring based topologies and following the reconfiguration process. Each node connects to the ring via two ports. In the normal state, two neighbouring nodes of the network become the Blocking State and cut off the connections logically between them to prevent loops. Each node monitors the neighboring segments including the blocking segment all the time. If any segment of the network is disconnected, it will be back to a normal state within a short recovery time by automatically moving the blocking segments to each end of the faulty part, thus isolating it.

- It broadcasts data to make each node have data, and it enables autonomous de-centered distributed process where each node can keep working even if network failure has occurred somewhere, and can achieve a high level of reliability.

- This use case describes the M2M Gateway which is a oneM2M MN and sends data received from real-time Ethernet.

- The oneM2M MN shall be able to transmit data according to priority in preparation for temporal performance degradation of underlying network, and for temporal increase of the amount of information data. The oneM2M MN shall also be able to identify series of data (e.g. time series data) and to indicate the individual data belonging to this series. With this function, the MN transmits data of each series with the same priority, even though the amount of one series of data temporally increases.

6.5.2 Source

- REQ-2015-0600R02: Real Time Data Collection.

6.5.3 Actors

- M2M Device: Sensors, controllers etc. located in factories (e.g. located at product lines) which measure and generate data. PLC/DCS control sensors in production lines according to embedded programs.

- Real-time Ethernet: In this use case, real-time Ethernet with the characteristics mentioned above is assumed. It is standardized in IEC TC 65 [i.21].

- oneM2M MN: The MN provides an interface from the real-time Ethernet to the oneM2M System. The oneM2M MN is developed as a dual Node (primary and secondary) to achieve a high-level of reliability.

- oneM2M Services Platform: The oneM2M services platform stores data gathered from MNs and provides data to applications.

- oneM2M Application: A oneM2M application in the Industrial Domain.

6.5.4 Pre-conditions

PLCs or DCSs send and receive data through real-time Ethernet.

6.5.5 Triggers

The primary MN and secondary MN receive data which is sent from PLCs or DCSs.

6.5.6 Normal Flow

1) The primary MN receives data and buffers it. If the buffer is overloaded then the data with the lowest priority is discarded.

2) The secondary MN also receives data and buffers it. If the buffer is overloaded then the data with the lowest priority is discarded.

3) The primary MN sends the buffered data with the highest priority to the oneM2M platform. If multiple data has the highest priority then the data flow of the least recent data transmitted is selected.

4) The secondary MN confirms the status of the primary MN and, as the primary MN is active, it stops the secondary MN from sending buffered data.

5) After a pre-defined time interval, the primary or secondary MN receives further data from either the PLCs or DCS.

6.5.7 Alternative flow

1) When the secondary MN confirms that the primary MN is not working the secondary MN sends buffered data.

2) After a pre-defined time interval, the secondary MN receives further data from either the PLCs or DCSs.

6.5.8 Post-conditions

When the process of sending data is not completed within the time interval, or the oneM2M platform does not receive the data, the primary or secondary MN sends the buffered data again.

6.5.9 High Level Illustration

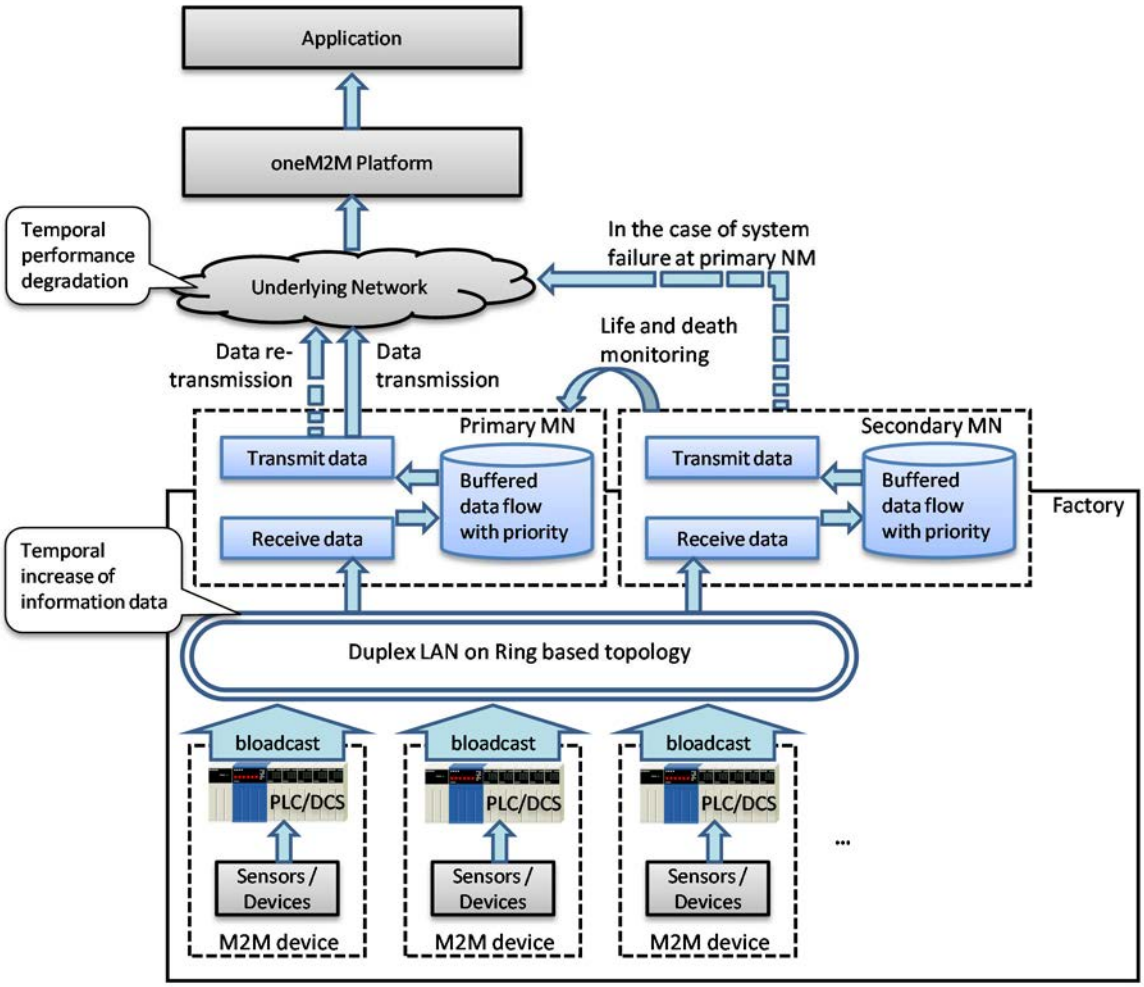


Figure 6.5.9-1: High-level Illustration of Real Time Data Collection

6.5.10 Potential Requirements

1) The oneM2M system shall be able to identify a series of data (e.g. time series data) and indicate the individual data belonging to this series.

2) The oneM2M system shall be able to transmit data according to priority (CRPR-003 [i.14]).

6.6 Data Encryption in Industrial Domain

6.6.1 Description

In smart factories data is essential for the execution of automation and efficient manufacturing. Data needs to be secured by measures such as authentication, authorization and encryption. As smart factories may connect to remote servers through multiple, partially external public networks, it cannot be assumed that these networks are secure. Encrypting data to avoid it being stolen in an external network and protecting the integrity of data to avoid it being modified is necessary for data security.

In the industrial domain the requirements of encryption are different (for example, sensitive data such as confidential commercial secrets need to be protected by strong encryption algorithms) and the capabilities of encryption/decryption vary for different devices (for example, for some low-cost devices, encryption/decryption with a long key may cause heavy loads to their poor processing units). Therefore each M2M application for smart factories needs proper encryption schemes to satisfy the various encryption requirements from application data while keeping the encryption/decryption loads acceptable to constrained devices.

M2M applications classify data into various levels based on the importance of the data and the capabilities of the devices. In the industrial domain the definition of sensitive data varies between products. For example, for manufactures of electric power grids, oil and gas, most data is sensitive since it includes confidential state secrets (required by governments to provide strong protection) while for makers of electronic products, information of product designs such as appearance or material is sensitive, since competitors stealing the product information will cause commercial damage. Based on common requirements from the industrial domain classification of application data is as follows, but not limit to, the categories below (dependent on M2M applications)

- **Sensitive data:** encryption strength is required (e.g. with longer key or electronic signature); sensitive data includes such as:
  - Confidential commercial secrets (e.g. customer information, intellectual properties, etc.).
  - Confidential data from infrastructure manufacturers (e.g. waveform data to diagnose, which is collected from devices in the power grid).
  - Data for industrial control systems (including filed bus, SCADA/Supervisory Control And Data Acquisition, controllers as PLC or DCS.
  - Keys transmitted for encryption algorithms.
- **Normal data:** encryption is recommended (optional) and proper applicable schemes should be adopted which are dependent on the capabilities of the devices; normal data includes such as:
  - Status data for product line and device monitoring (e.g. device availability) in normal products manufacture which do not include any commercial secrets.
  - Data for human resources monitoring and employee performance assessment (e.g. GPS information of workers collected from carried mobile tablets).

When various levels of application data in industrial domain is encrypted /decrypted based on its associated encryption scheme, the essential data is secured and the loads caused by normal data encryption are acceptable for constrained devices.

6.6.2 Source

- REQ-2015-0603R03: Data encryption in industrial domain.

6.6.3 Actors

M2M Device: Machines, sensors, controllers etc. located in factories which measure and generate data. PLC /DCS control machines and sensors in production lines according to embedded programs.

Intra-factory Network: In this use case, the intra-factory network is assumed to be managed by factory owners (different from the Underlying Network operated by external parties).

oneM2M MN: The MN collects data from the intra-factory network and sends the data to the oneM2M services platform through underlying network.

oneM2M Services Platform: Support secure data transmission and mapping of application data levels to applicable encryption schemes.

oneM2M Application: Classify data based on sensitivity.

6.6.4 Pre-conditions

The oneM2M Services Platform and security CSE inside M2M devices/MNs support various application data levels and mapping these levels to applicable encryption schemes.

6.6.5 Normal Flow

1) The M2M application classifies data into various levels (e.g. into sensitive data and normal data).

2) The oneM2M Services Platform or security CSE inside M2M devices/MNs maps these levels to applicable encryption schemes.

3) Each pair of transmitter and receiver performs preparation procedure (e.g. share symmetric key and store it in respective storage inside nodes) before sending encrypted data.

4) The transmitter (e.g. a server located at one end of the application) prepares the data for sending; encrypts the data based on its associated security level (with respective encryption algorithm, key length etc.).

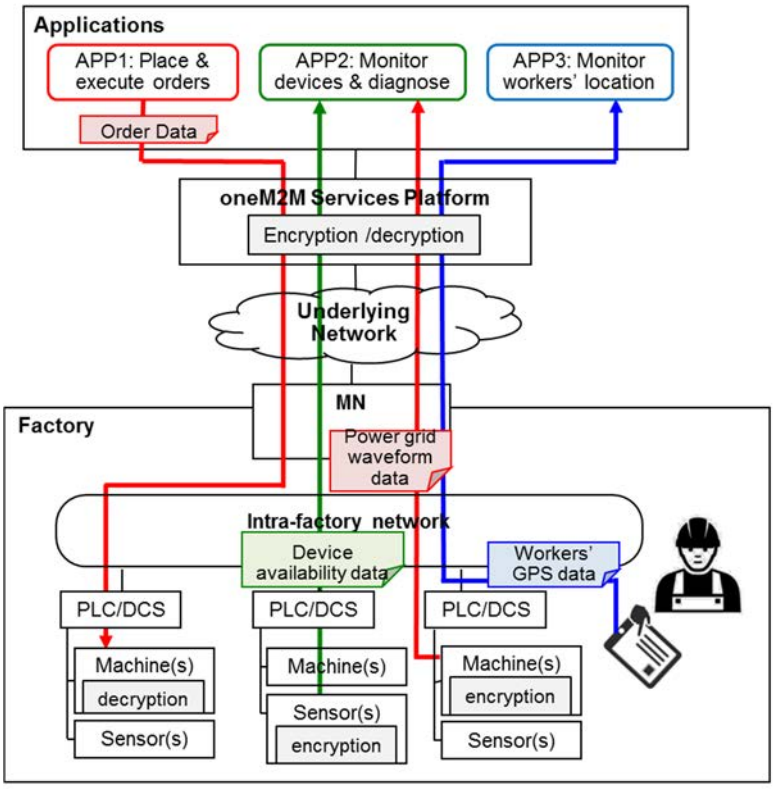
5) The encrypted data is sent to the receiver through intra-factory network and public underlying networks.

6) The receiver (e.g. a machine located at the other end of the application) receives the data from transmitter and decrypts the data.

6.6.6 Post-conditions

The M2M application utilizes the decrypted data for smart manufacturing, such as executing orders, monitoring devices and diagnosis, monitoring workers' location, etc.

6.6.7 High Level Illustration



Example of mapping application data levels to encryption schemes

Security levels	Application Data type	Encryption algorithms (Spec: FIPS Pub 197)
High	Order data, Power grid waveform data	AES-256
Normal	Device availability data	AES-128
Low	Worker's GPS data	No encryption

Figure 6.6.7-1: High-level Illustration of Real Time Data Collection

6.6.8 Potential Requirements

1) The oneM2M system shall support classification of application data by oneM2M applications into various security levels that are specified by oneM2M and support the mapping of these levels to applicable security capabilities.

6.7 Qos/QoI Monitoring in Industrial Domain

6.7.1 Description

In factories a lot of data are generated from M2M devices (e.g. machines and program logic controllers) and the data are delivered to the M2M gateway via industrial bus systems, e.g. Real-time Ethernet. In addition, factory management applications can get factory status information through the oneM2M Service platform (Infrastructure Node) which gathers data from M2M gateways located in each factory domain.

In local industrial communications data packet transmission between M2M gateway and M2M devices has real-time transmission characteristic delivered over an Ethernet-based communication system. However to enable remote mechanisms (remote supervisory, operation, service), Wide Area Networks is composed of broad and heterogeneous communication technologies, e.g. digital wireless telecommunication systems (GSM-based, UMTS-based), digital wired telecommunication systems (ISDN, DSL).

In this environment the M2M gateway can use various telecommunication systems to send and receive data packets from the oneM2M service platform. In addition, according to industrial application service types, it requires hard real-time data delivery, soft real-time data delivery or real-time not requiring data delivery when it comes to communication between the M2M gateway and the oneM2M service platform.

If Quality of Service (QoS) required from the application can not be guaranteed, this situation limits service scenarios in industrial domains. In order to prevent this situation, the M2M gateway can decrease the volume of data needed to send the oneM2M platform via data processing based on data catalogue. At the same time, if the M2M gateway can monitor network environments, it can dynamically choose the network type or network provider who guarantees the required QoS.

In addition, to satisfy QoS, real-time data generated from M2M devices can be pre-processed/filtered, based on the data catalogue. In this situation, post-processed data is to include a kind of Quality of Information (QoI) and if QoI monitored and delivered to the oneM2M service platform, this information can be used for further data processing in the oneM2M platform.

This use case proposes that the oneM2M system offers QoS/QoI Monitoring capabilities, which includes data accuracy, data age, cost, communication, encryption, etc.

6.7.2 Source

- REQ-2015-0606R01: QoS/QoI monitoring in industrial domain.

6.7.3 Actors

- M2M Devices: Sensors, controllers etc. located in factories (e.g. located at product lines) which measure and generate data. PLC /DCS control sensors in production lines according to embedded programs.
- Real-time Ethernet: A technology standardized in IEC TC 65 [i.21] for use in industrial control system.
- MN Gateway (MN): It provides an interface from the Real-time Ethernet to the oneM2M system. The gateway collects data from M2M devices which are connected via Real-Time Ethernet communication technology. The gateway can conduct data pre-processing/filtering based on the data catalog delivered from the oneM2M service platform.
- oneM2M Service Platform (IN): It acts as a oneM2M Infrastructure Node. It communicates with MNs in the remote industrial domains and gathers the data from the MN. The data in the oneM2M service platform can be delivered to the applications, e.g. factory monitoring application.
- Applications: An M2M application in the application service provider domain. It monitors production lines and sends analyzed results or alert messages to the factory administrator.

6.7.4 Pre-conditions

- Devices (e.g. PLC, Machines) and the gateway are connected to Real-time Ethernet. PLCs broadcast data to Real-time Ethernet.
- The Gateway can have a capability of various network hardware interfaces (e.g. GSM-based, UMTS-based, ISDN, DSL) and can also use various network service providers who guarantee the required QoS level.

6.7.5 Triggers

- The Application initiates service which require QoS/QoI requirement (e.g. response time, data freshness).
- The Application sends the QoS/QoI requirement to oneM2M platform.

6.7.6 Normal Flow

- The oneM2M service platform requests QoS/QoI monitoring data from the MN and based on this information, the oneM2M service platform negotiates the supported QoS/QoI parameter with the application.
- To enable end-to-end services, the oneM2M service platform sends the QoS requirement to the MN. Based on the QoS requirement, the MN dynamically chooses the network type and network service provider who guarantees the required QoS level.
- In the MN, the QoS/QoI monitoring function can annotate data with quality information.
- After receiving data from the MN, the oneM2M service platform can further process the data referring to the quality attributes.

6.7.7 Alternative flow

None.

6.7.8 Post-conditions

None.

6.7.9 High Level Illustration

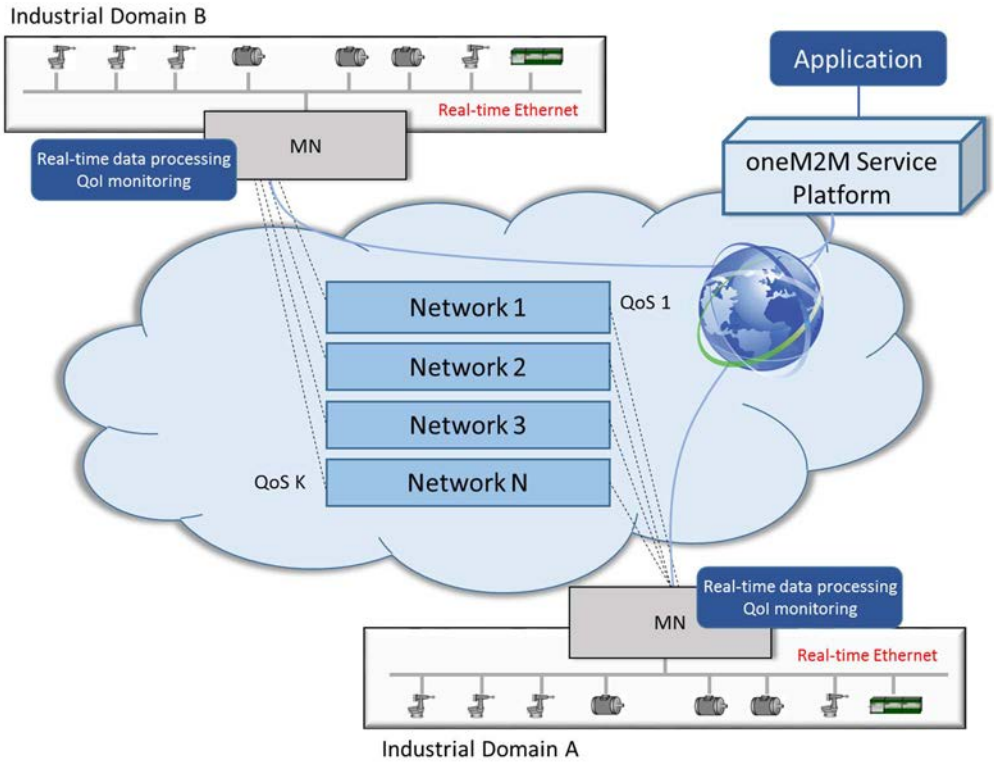


Figure 6.7.9-1: High-level Illustration of QoS/QoI Monitoring in Industrial Domain

6.7.10 Potential Requirements

1) The oneM2M System shall support the inclusion of M2M Application's QoS preference in service requests to Underlying Networks (OSR-038 [i.14]).

2) The oneM2M System shall provide the capability to monitor and describe data streams with associated attributes, e.g. data freshness, accuracy, sampling rate, data integrity.

7 Overview of Potential Requirements

Potential requirements from all industrial use cases collected in this technical report are summarized as follows:

1) The oneM2M System shall be able to collect data that is broadcast (e.g. in industrial bus systems) according to data collection policies (OSR-081 [i.14]).

NOTE 1: This requirement addresses the use case 6.1 "An industrial use case for on-demand data collection for factories".

2) The oneM2M System shall allow the update, modification, or deletion of data collection policies within an M2M application (OSR-082 [i.14]).

NOTE 2: This requirement addresses the use case 6.1.

3) The oneM2M System shall be able to collect, store time series data (OSR-075 [i.14]).

NOTE 3: This requirement addresses the use case 6.2 "Integrity of Data Collection Monitoring".

4) The oneM2M System shall be able to detect and report the missing data in time series (OSR-076 [i.14]).

NOTE 4: This requirement addresses the use case 6.2.

5) The oneM2M System shall be able to support receipt of the status information of the Underlying Network if supported by the Underlying Network (OPR-007 [i.14]).

NOTE 5: This requirement addresses the use case 6.2.

6) The oneM2M System shall be able to provide the M2M applications with status information received from the Underlying Network (OPR-008 [i.14]).

NOTE 6: This requirement addresses the use case 6.2.

7) The oneM2M System shall be able to share data collection policies among multiple M2M Devices/Gateways within an M2M application service, or among different M2M application services (OSR-097 [i.14]).

NOTE 7: This requirement addresses the use case 6.3 "Data Process for Inter-factory manufacturing".

8) The oneM2M System shall be able to support mechanism for the M2M Devices and/or Gateways to report their geographical location information to M2M Applications (OSR-047 [i.14]).

NOTE 8: This requirement addresses the use case 6.4 "Aircraft construction and maintenance".

9) The oneM2M System shall support the ability for single or multiple M2M Applications to interact with a single or multiple M2M Devices/Gateways (application in the device/gateway) (OSR-009 [i.14]).

NOTE 9: This requirement addresses the use case 6.4.

10) The oneM2M System shall be able to identify a series of data (e.g. time series data) and indicate individual data belong to this series (CMR-015 [i.14]).

NOTE 10: This requirement addresses the use case 6.5 "Real Time Data Collection".

11) The oneM2M System shall be able to transmit data according to priority.

NOTE 11: This requirement addresses the use case 6.5 and it is included in/supported by CMR-003 [i.14].

12) The oneM2M System shall support classification of application data by oneM2M applications into various security levels that are specified by oneM2M and support the mapping of these levels to applicable security capabilities (SER-045 [i.14]).

NOTE 12: This requirement addresses the use case 6.6 "Data Encryption in Industrial Domain".

13) The oneM2M System shall support the inclusion of M2M Application's QoS preference in service requests to Underlying Networks (OSR-038 [i.14]).

NOTE 13: This requirement addresses the use case 6.7 "QoS/QoI monitoring in industrial domain".

14) The oneM2M System shall provide the capability for monitoring and describing data streams with associated attributes e.g. data freshness, accuracy, sampling rate, data integrity (OSR-092 [i.14]).

NOTE 14: This requirement addresses the use case 6.7.

8 High Level Architecture

8.1 Introduction

The seven use cases in the industrial domain discussed in the present document are listed in table 8.1-1.

Table 8.1-1: Use cases in the industrial domain

Use case No.	Title	Description
1	An industrial use case for on-demand data collection for factories	See clause 6.1
2	Integrity of data collection monitoring	See clause 6.2
3	Data process for inter-factory manufacturing	See clause 6.3
4	Aircraft construction and maintenance	See clause 6.4
5	Real Time Data Collection	See clause 6.5
6	Data encryption in industrial domain	See clause 6.6
7	QoS/QoI monitoring in industrial domain	See clause 6.7

The deployments which support these use cases require the use of M2M Devices which use broadcasting mode through the PLC or DCS. The following clauses provide the high level oneM2M architecture mapping for these deployments.

8.2 Deployment Mapping Using IPE

Table 8.2-1 lists the mapping relationship between the actors in industrial domain and the nodes in oneM2M domain. Those devices under the M2M Gateway are non-oneM2M devices which can be mapped into the M2M Area Network. In this case, the M2M Gateway which is mapped to the MN shall implement the Inter-working Proxy Application Entity (IPE).

Table 8.2-1: Mapping relationship 1

Use case No.	Actors in the use case	oneM2M Node
1, 2, 3, 4, 5, 6, 7	Application and M2M service platform	IN
1, 2, 3, 5, 6, 7	M2M Gateway	MN
	M2M Devices (PLC/DCS, sensors) and Intra-factory network	Non-oneM2M Device in M2M Area Network
4	WiFi gateway	MN
	Power tools and underlying network (WiFi)	Non-oneM2M Device in M2M Area Network

Figure 8.2-1 illustrates Deployment Mapping Using IPE.

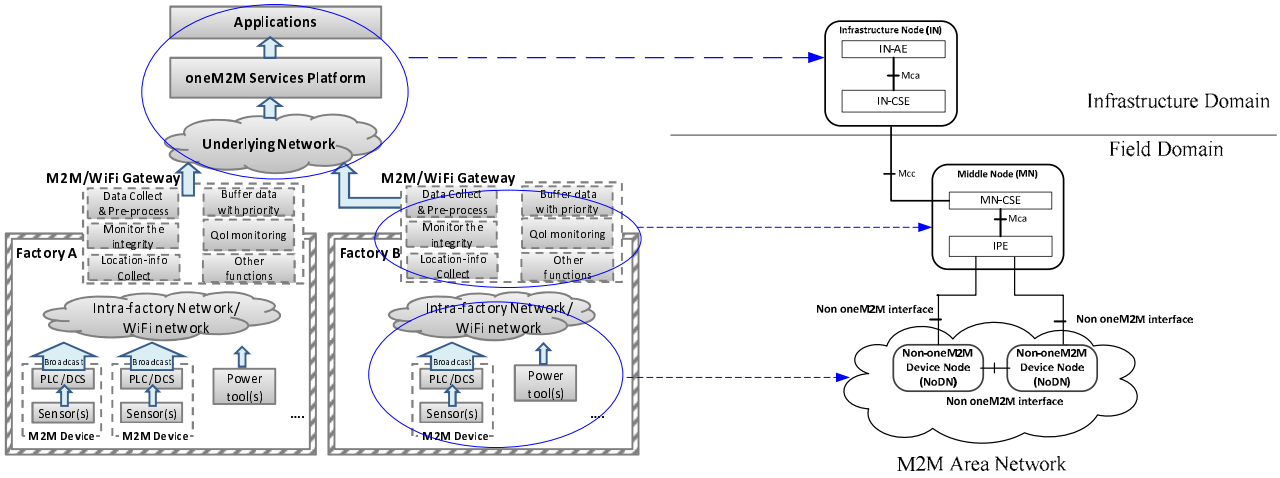


Figure 8.2-1: Deployment Mapping Using IPE

8.3 Deployment Mapping Using Peer-to-Peer Communication

Table 8.3-1 lists the mapping relationship between actors in industrial domain and nodes in the oneM2M domain. In this case, all of the actors are assumed to be oneM2M compliant nodes.

Table 8.3-1: Mapping relationship 2

Use case No.	Actors in the use case	oneM2M Node
1, 2, 3, 4, 5, 6, 7	Application and M2M service platform	IN
1, 2, 3, 5, 6, 7	M2M Gateway	MN
	M2M Devices (PLC/DCS, sensors)	ADN/ASN
4	WiFi gateway	MN
	Power tools	ADN/ASN

Figure 8.3-1 illustrates Deployment Mapping for Peer-to-Peer Communication. In the existing factory production line, M2M Devices with PLC/DCS will support peer-to-peer communication, which means data can be exchanged among nodes directly. Note that peer-to-peer communication between CSEs of different ASNs is currently not supported by oneM2M architecture deployment (see clause 6.1 of ETSI TS 118 101 [i.15]).

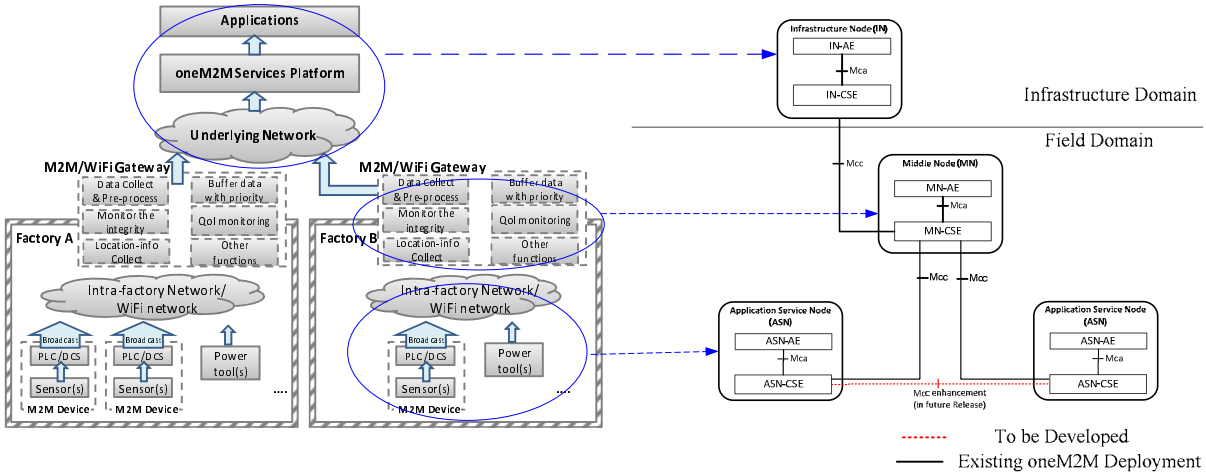


Figure 8.3-1: Deployment Mapping Using Peer-to-Peer Communication

8.4 Conclusion

Since M2M Devices with PLC/DCS need to support peer-to-peer communication, the existing reference enhancement between CSEs of different ASNs shall be considered in the future oneM2M releases.

9 Security Analysis

9.1 Introduction

The use cases in clause 6 have described three categories of smart manufacturing scenarios which include "inside the factory", "collaborated factories" and "factories connected to remote server/center". In these scenarios, devices are deployed in multiple networks which construct the factories (such as enterprise network, control system network, supervisory network, field network etc.) and these networks are connected by various types of boundary nodes. The factories also increase connectivity to the outside for remote facility, data center or remote smart manufacturing services. Therefore, cyber attackers have plenty of opportunities to access a manufacturer's trade secrets and sensitive production data, or attack against important industrial systems (e.g. control system).

Compared to other vertical domains, the industrial domain has some specific characteristics which may impact the security requirements, such as:

- **Real-time:** This characteristic is also known as "timely response to events" in industrial domain. For some devices inside the factory, their tasks need to be processed within a certain period of time, especially the sensing and actuating devices in Industrial Automation & Control System (IACS).
- **Various protection motivations & different device capabilities:** In different industrial systems, the motivation for protection may vary (from normal to high) depending on the importance of asset or data. The capabilities of device may also vary, which means they may provide different resources or complexity of protection mechanisms. Therefore a mixed mode of protection solutions is usually required in practical industrial scenarios.
- **Co-existence of multiple networks:** In the above three categories of industrial scenarios, industrial Ethernet/ fieldbus and enterprise WLAN are deployed for inside factory scenarios; public internet is the necessary network for connecting one factory to another or to remote center.

Considering these characteristics in the industrial domain, some international standard organizations have made industrial security standards. For example, IEC have made the 62443 series as the standards for IACS and defined 4 security levels (SLs) based on various security motivations and device capabilities [i.16]. (SL0 is defined as no security requirements; from SL1 to SL4, the motivation for protection, consumed resources and complexity of protection mechanisms increase; for SL3 and SL4, IACS specific skills are possibly utilized.)

The foundational security requirements in the industrial domain are detailed in the clauses from 9.2 to 9.6.

9.2 Identification and Authentication

All users (humans, devices and software processes) need to be identified and authenticated before allowing them to access certain systems for operating devices or acquiring data.

The Identification and Authentication function defined in ETSI TS 118 103 [i.17] is in charge of identification and mutual authentication of CSEs and AEs. If all the actors in the industrial domain are oneM2M compliant nodes, defined mechanisms in ETSI TS 118 103 [i.17] are possibly used to identify and authenticate any access request. Methods include using passwords, tokens or location (physical or logical), and are not limited to other feasible methods.

9.3 Use Control

9.3.1 Introduction

Once the user is identified and authenticated, the industrial domain has to restrict the allowed actions to the authorized use of the targeted devices/resources. If a requested operation is covered by the permissions accorded by the Access Control Policies (ACPs), the operation is executed, otherwise it is rejected.

The requirement of use control also includes session lock which is required to prevent access after a period of inactivity and the limitation of concurrent sessions which is required for DoS prevention.

9.3.2 Authorization

Similarly with the definition of Authorization function in ETSI TS 118 103 [i.17], services and data access in the industrial domain are authorized to authenticated entities/users according to provisioned ACPs and assigned roles. Identity-based ACP (Access Control List in ETSI TS 118 103 [i.17]), role-based ACP (RBAC in ETSI TS 118 103 [i.17]) and rule-based ACP are the common authorization mechanisms.

An additional requirement of supervisor override exists in the industrial domain. While automated common authorization mechanisms are sufficient in most scenarios, in the event of emergencies or other serious events, a manual override of automated authorization mechanism is needed, especially in control systems.

9.3.3 Session Lock & Concurrent Session Control

Session lock: The industrial control system may require the prevention of further access by initiating a session lock after a configurable time period of inactivity or by manual initiation (although the previous action has been authorized according to the ACP).

Concurrent session control: The industrial control system may require the limitation of the number of concurrent sessions per interface, for any given user to a configurable number of sessions. A resource starvation DoS might occur if a limitation is not imposed.

9.4 Data Confidentiality

9.4.1 Introduction

The sensitivity and the importance of data in industrial domain may be diverse (see clause 6.6 for classification of application data in industrial domain). In the case of some control system-generated data, for example, (whether at-rest or in transit), this kind of data may be of a confidential or sensitive nature, therefore data storage and communication channels should be secure.

Based on the various protection motivations (depending on the sensitivity of the data) and the different device capabilities, different industries may require different levels of encryption strengths for each data category. The use of cryptography is required to match the value of data, the time period during which the data is confidential and industrial constraints. The industrial control system should utilize encryption and hash algorithms such as AES, SHA series, and key size based on generally accepted practices and recommendations [i.18].

In addition to the common cryptography mechanisms, there are other security solutions needed to meet specific industrial requirements which are detailed in the clauses 9.4.2 and 9.4.3.

9.4.2 Light-weight Encryption

Standard applications of data encryption algorithms do not always meet real-time processing requirements. Within a packet, data at different positions may have various levels of importance, and consequently different security level needs. Therefore, using a low security level of data encryption at specific positions may be used to avoid unnecessary processing overhead. For example, the best practice might be for a light-weight encryption procedure to be used for efficient and highly automated devices used in control systems.

A simple encryption procedure is provided by ITU-T [i.19], which significantly reduces the consumed time for encryption and meanwhile protects data confidentiality and integrity. Such light-weight encryption algorithms shall be considered for protecting industrial data, especially for low-cost devices.

9.4.3 Session Based Encryption

To exchange very sensitive data (such as manufacturer's trade secrets and sensitive production data), a session key shall be used for secure sessions. The defined Security Association Establishment procedure in ETSI TS 118 103 [i.17] results in a TLS or DTLS session which protects the data via a secure session establishment. Such a secure connection shall be established to protect the confidential and sensitive data in industrial domain.

9.5 System Integrity

9.5.1 Introduction

The capability to protect system integrity is required in the industrial domain, especially for the protection of communication integrity and session integrity.

9.5.2 Communication Integrity

Many attacks are based on the manipulation of data in transmission. Manipulation in the context of a control system could include the change of measurement values communicated from a sensing device to a receiver, or the alteration of command parameters sent from a control application to an actuating device.

The Message Integrity Code (MIC) is defined in ETSI TS 118 103 [i.17] to provide integrity protection for the exchange of messages across reference points. Such cryptographic mechanisms shall be provided to protect the integrity of data in transmission for the industrial domain.

9.5.3 Session Integrity

Besides protecting data in transmission, the integrity of sessions also needs protection in the industrial domain. This integrity focuses on the protection at the 'session versus packet' level (such as prevent session hijacking, insertion of false information into a session). The intent is to establish confidence at each end of a communication session in the ongoing identity of the other party. Use of session integrity may lead to significant overhead and therefore the use should only be considered when real-time communication is required.

9.6 Restricted Data Flow

Some important industrial systems (e.g. control systems) may be disconnected from an enterprise network or public network using unidirectional gateways, stateful firewalls and DMZs to manage the flow of data.

As the co-existent multiple networks in the industrial domain are connected by boundary nodes, these boundary nodes such as gateways, proxies, firewalls shall provide proper capabilities to restrict or prohibit network access in accordance with provisioned security policies and an assessment of risk.

9.7 Conclusion

Considering the specific security requirements and the best practices of the industrial domain enhancement of security solutions shall be considered in the future oneM2M releases.

10 Conclusion

The use cases of the industrial domain mainly include the communication and interaction of intra-factory and inter-factory scenarios, in which, effective collaboration between factories is achieved based on the connectivity provided by M2M technologies, and collected field data from all factories is used to make accurate decisions and timely responses. These use cases need the oneM2M system to support the requirements such as collecting field data from factories and supporting new data types (e.g. time series data), monitoring the status of underlying network to satisfy the QoS of applications, and classifying application data into various security levels.

To support the above use cases and requirements of industrial domain by oneM2M common service layer, industrial domain systems are integrated with oneM2M architecture. Additionally the enhancement of oneM2M architecture shall be considered, such as introducing new resource types for implementing time series data and enhancing existing reference between CSEs of different ASNs to support peer-to-peer communication for manufacturing requirements. These functionalities need to be taken into account in future oneM2M specifications in order to deploy industrial service based on oneM2M system.

Additionally, specific security requirements are summarized. For the best practice of deploying industrial services, the enhancement of existing security solutions shall be considered in future oneM2M specifications, such as supporting end to end security and classifying application data into various security levels.

History

Document history		
V2.0.0	September 2016	Publication