Automaatiopäivät[22] 2016 Seminar:
Using OPC Unified Architecture to Enable Secure Industrial Internet Solution

Jouni Aro
Prosys PMS Ltd, Tekniikantie 14, FI-02150 Espoo, Finland
Tel: +358 50 5050 313, E-mail: jouni.aro@prosysopc.com, http://www.prosysopc.com

KEY WORDS: Standardization, Industrie 4.0, Smart Factory, Security, Industrial Internet

ABSTRACT

OPC Unified Architecture (OPC UA, IEC 62541) is becoming the communication standard for Industrial Internet solutions. The German Platform Industrie 4.0 has defined it to be the communication protocol of choice for the Reference Architecture Model for Industrie 4.0 (RAMI 4.0). The German Federal Office for Information Security (BSI) has evaluated OPC UA and recommends it for industrial environments because of the built-in security mechanisms.

1 BACKGROUND

OPC has a strong background in industrial automation systems as an interoperation protocol since 1990's. OPC defines a generic interface standard for exchanging measurement information: current values, alarms and historical data (i.e. trends) between various systems. The "Classical OPC" is a de facto standard in production automation, but it has several practical limitations to make it a widely adopted communication protocol.

OPC Unified Architecture is the second generation of the protocol. It has been designed from grounds up to replace the "Classical OPC" with a robust, high-performance, secure protocol that is platform independent. It enables flexible integration of different systems that are dealing with measurement data, including current values, alarms and historical data – and extends to incorporating various existing information models, such as IEC 61131-3 (PLCopen), ISA-95, AutomationML, etc.

2 INDUSTRIE 4.0

Reference Architecture Model for Industrie 4.0 (RAMI 4.0) is a complete architecture model for future manufacturing processes, including product life-cycle management (based on IEC 62890), production hierarchy levels (based on IEC 62264/ISA-95 and IEC 61512/ISA-88) and different business layers. The model is based highly on various existing standards and OPC UA is selected as the standard communication protocol for the model. OPC UA has the capability to standardize the connectivity between all manufacturing automation systems.

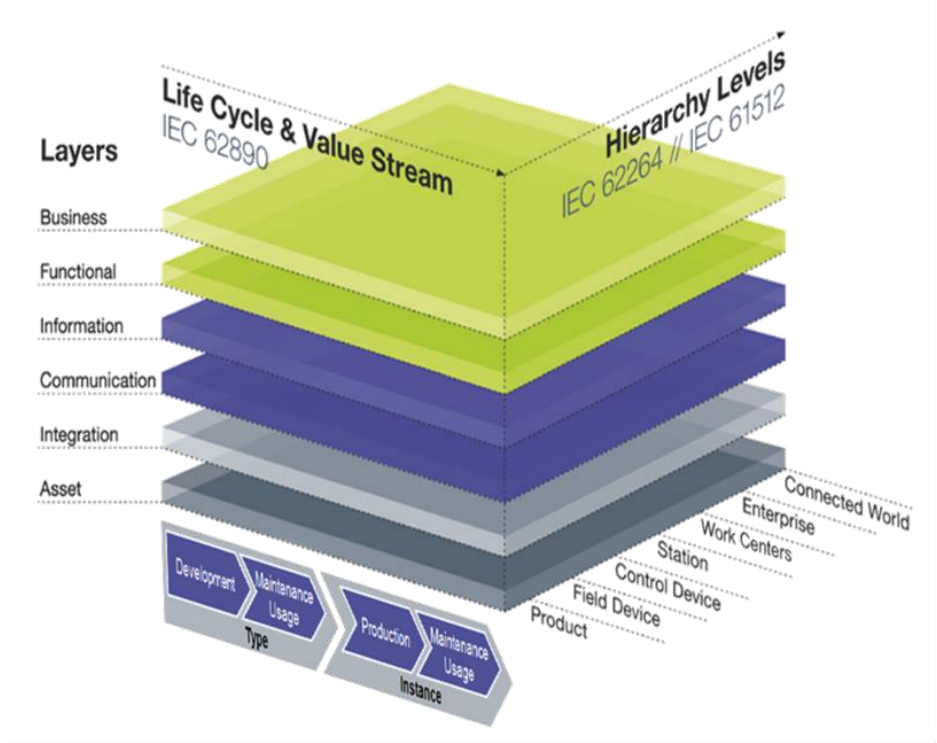

Figure 1. Reference Architecture Model for Industrie 4.0 (RAMI4.0) ensures that all participants involved in Industrie 4.0 discussions understand each other. /1/

RAMI 4.0 is also defining a concept of an Industrie 4.0 component. /1/ The concept defines an "enhanced product", where an Administration Shell is surrounding any physical component that can be connected to the Industrie 4.0 compatible environment. The Administration Shell is a software component that enables configuration and management of life-cycle data for the physical component. OPC UA will provide the standard communication for the Administration Shell. The Administration Shell conforms to the standard for the Digital Factory, IEC 62832 CD2 Part 1,which "defines a framework of abstract definitions for Assets of automated systems, Structural and behavioural relationships, Feature (property) management, Hierarchical relationships and Technical aspects" /1/.

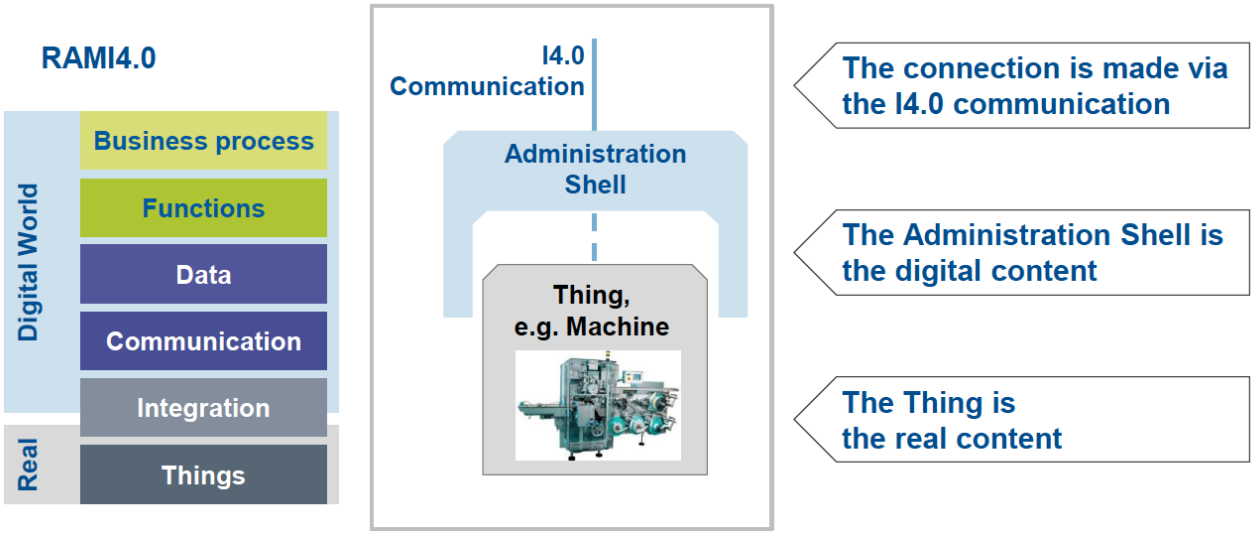

Figure 2. The Administration Shell defines a digital interface to physical things. /2/

Other international organizations, such as Industrial Internet Consortium and Made in China 2025 are following the progress of Industrie 4.0. The reference architecture models of these programs are being synchronized with the RAMI 4.0. This may lead to a globally standard model.

3 SECURITY

OPC UA defines an abstract communication model, enabling different transport protocols. It also defines a specific optimized binary protocol, which is used by most applications. Each alternative protocol enables high level of security. Applications are authenticated with PKI certificates and you can build a trust network between the applications that may connect to each other. All communication can be optionally encrypted using symmetric AES-128 or AES-256 algorithms. A more specific description of the security mechanisms is given in (Aro-Tahvanainen 2015).

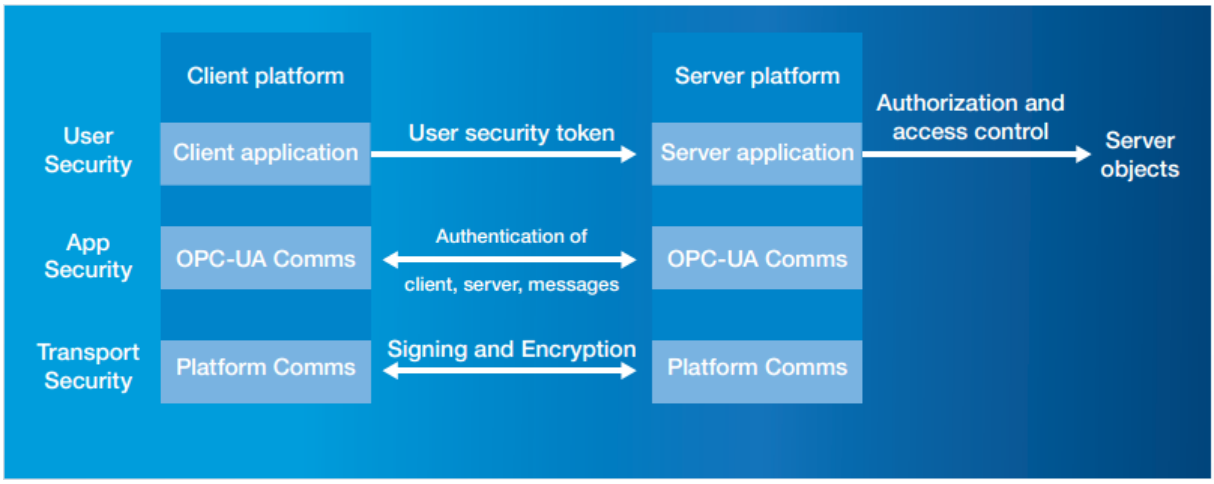

Figure 3. OPC UA Security Model /3/

4 COMMUNICATION MODEL

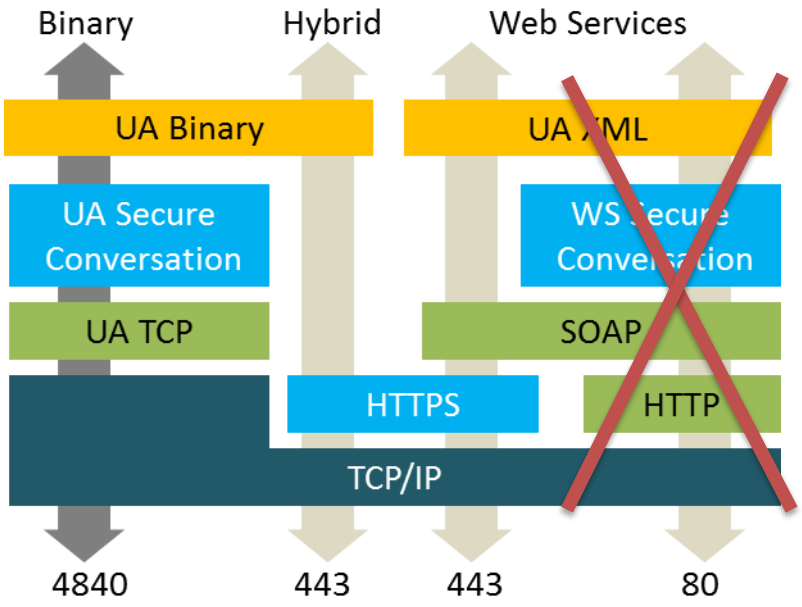

Figure 4. OPC UA Communication Model. Modified from /3/

The standard OPC UA communication model is a session-based client/server –model. Server applications provide data for client applications, which can read and write data from the servers. The clients may also subscribe to data changes or events independent of each other.

The abstract communication model is mapped into various implementations using existing protocols (such as HTTPS) and a custom high-performance protocol (UA TCP). In future, both the protocols and security profiles can be extended flexibly.

4 PUBLISHER/SUBSCRIBER MODEL

In addition to the traditional Cleint/Server-model, OPC Foundation has been defining a new communication model that will suit other use cases in future. The Publisher/Subscriber model defines two alternative communication models:

- message queue and
- secure multicast model.

The message queue based protocol enables more flexible subscription in wider networks, especially for cloud systems. The servers will publish data to a message broker and clients can subscribe to the data that is made available. The message queue enables more robust communication without specific sessions.

The Secure Multicast model is based on UDP broadcasting. In this model the server is broadcasting selected data changes to a local network where all clients that wish to subscribe to the data can listen to the changes. This will enable more efficient delivery with slower latencies. OPC Foundation is also co-operating with the Time-Sensitive Networking Task Group that is building new standards that would enable hard real-time requirements on top of standard Ethernet (IEEE 802.1) networks.

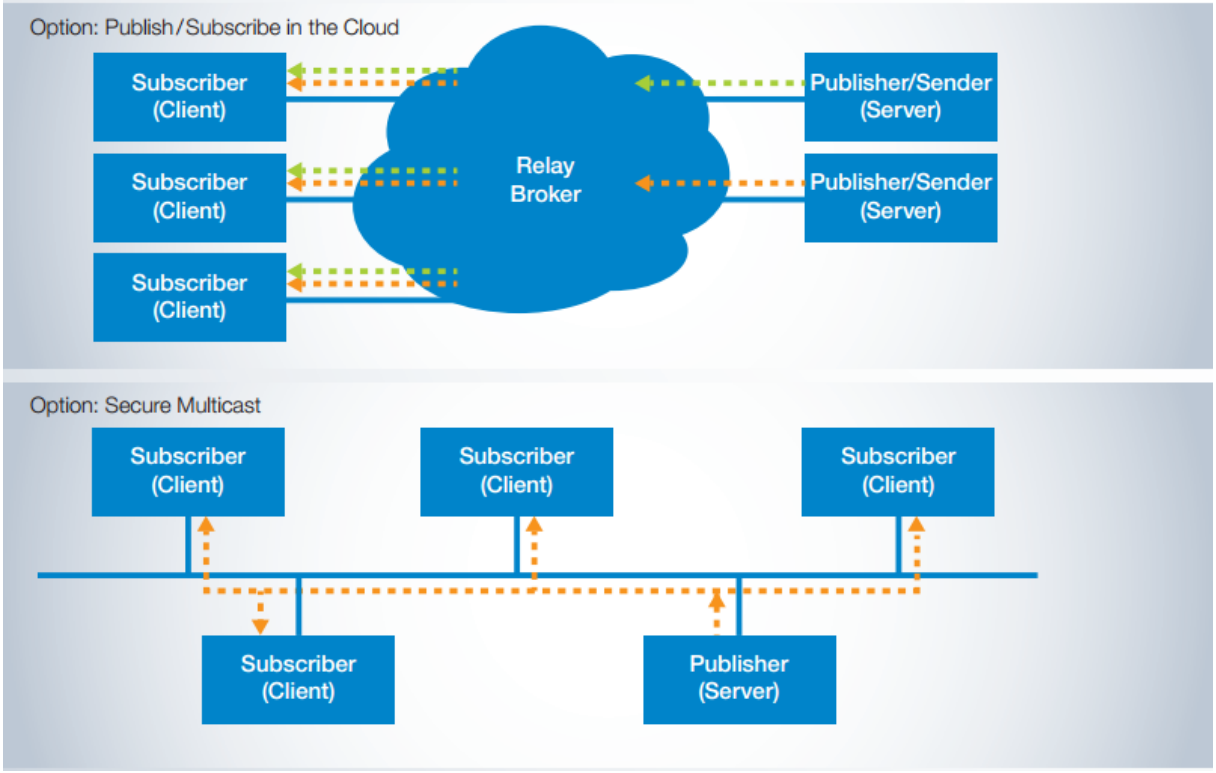

Figure 5. OPC UA Publisher/Subscriber protocols /3/

5 INFORMATION MODELING

The generic communication models enable secure interoperability between applications on the communication level. To raise the interoperability to the semantic level, OPC Foundation has also defined a standard information modeling concept. This enables standard information types, such as various device and machine types to be modelled with OPC UA. And this consequently, enables applications to be integrated on the information level, in addition to the secure communication level.

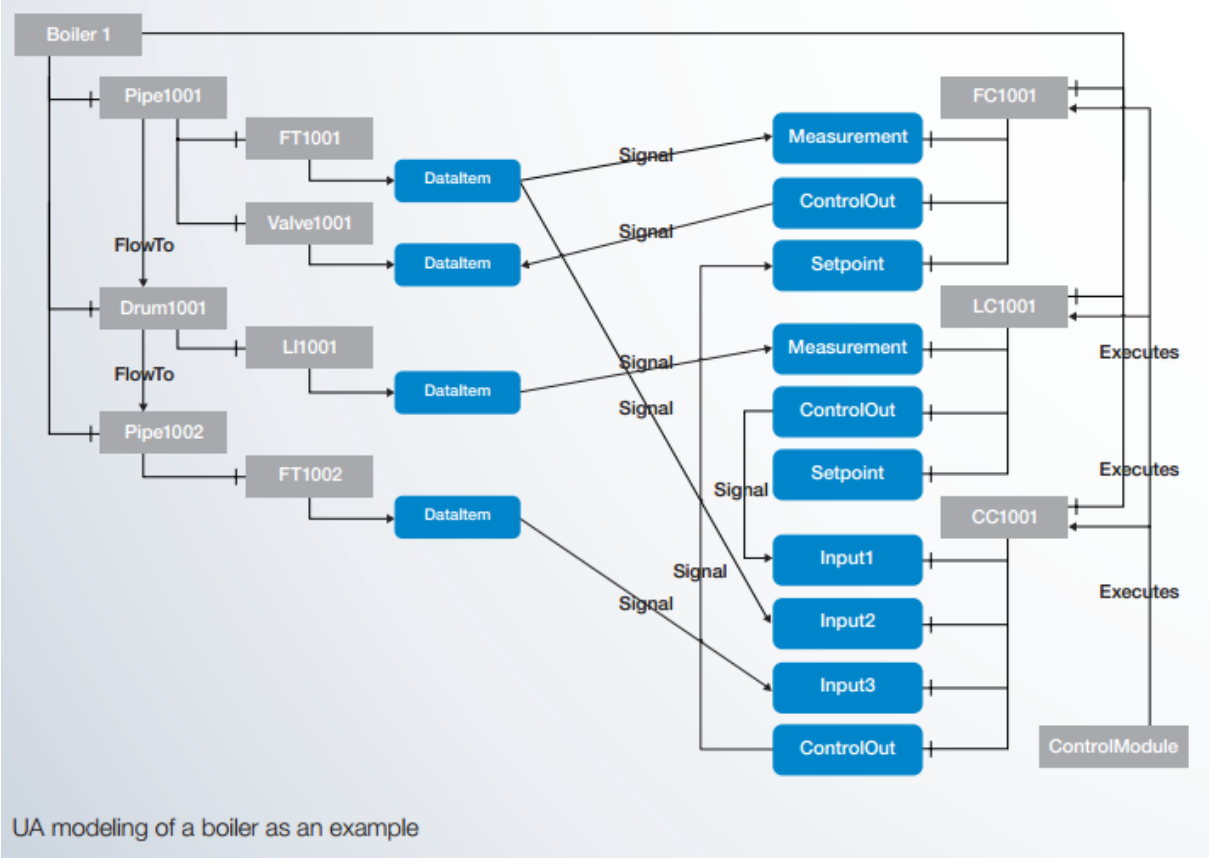

Figure 6. A sample OPC UA Information Model /3/

6 COLLABORATION

OPC Foundation is collaborating with all major standardization organizations that are defining information models, to also incorporate the existing models to OPC UA. This makes OPC UA capable of providing a standard means to communicate various information models through the same channel and therefore integrating different systems and information models together. This makes OPC UA a truly unique platform for the Industrial Internet.

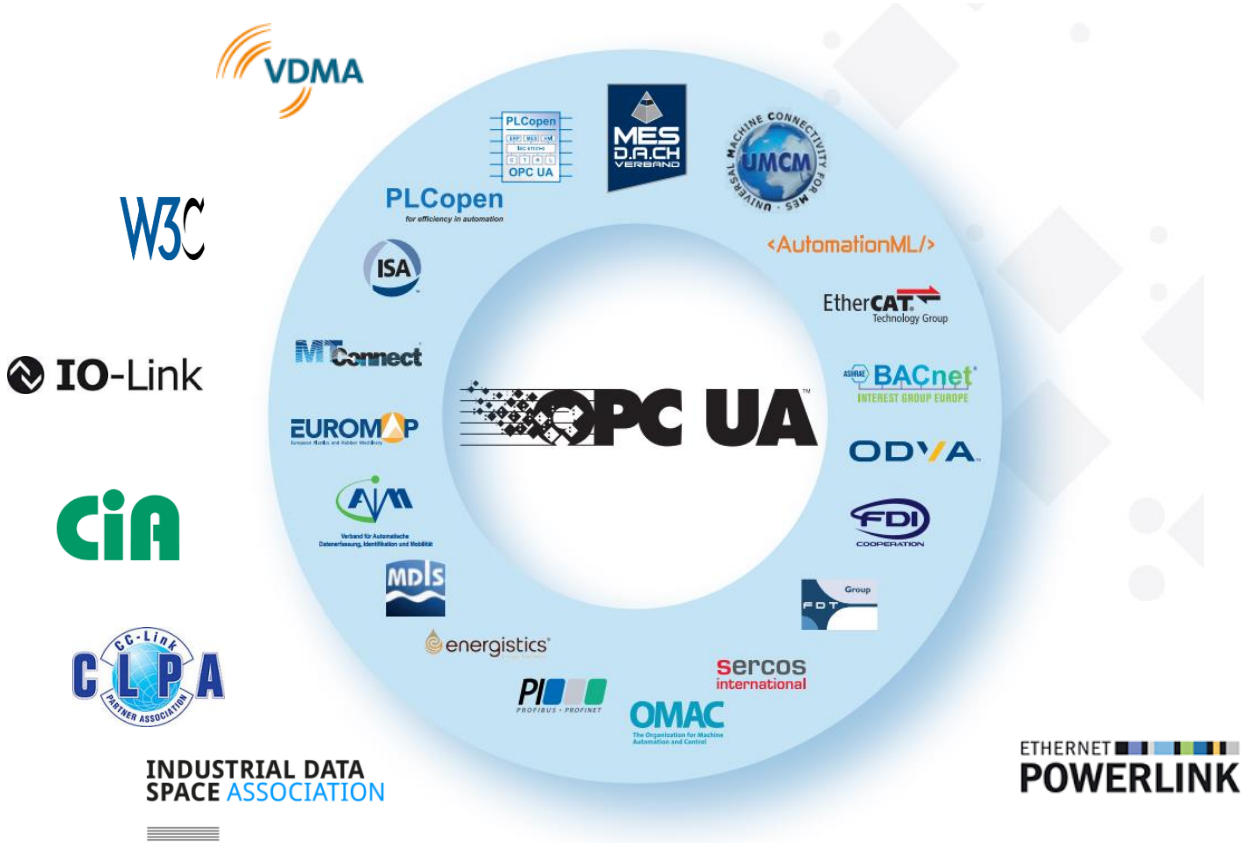

Figure 7. OPC Foundation has built a wide collaboration network, targeting to bring all major information models into OPC UA.

7 JAVA FRAMEWORK FOR OPC UA

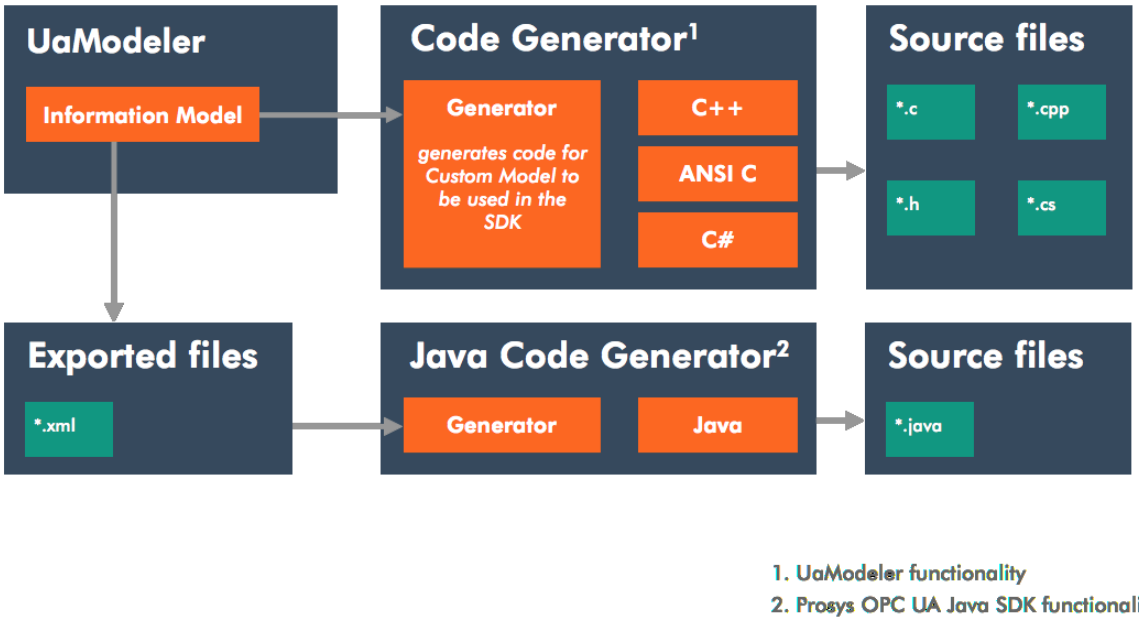

Figure 8. UaModeler helps to create the Information models, which can then be also generated to various source code classes as well.

Prosys OPC UA Java SDK provides a first class library for developing OPC UA applications in Java. The 100% Java implementation of the OPC UA communication protocol and a high-level application programming interface (API) provide a solid basis for building secure and reliable applications and software components for

the needs of Industrial Internet. The SDK includes a code generation capability /6/, which enables any OPC UA information model to be converted to Java classes that are easy to use in development. The information models enable integration of systems and components on a semantic level, in addition to pure communication level. The code generated classes ensure a true Java API for using the information models in all types of OPC UA applications.

8 OPC UA GATEWAY TO MODBUS NETWORKS

An example of enabling secure integration of existing communication networks, is provided by the OPC UA Modbus Server, which can act as a gateway between OPC UA and Modbus TCP/IP networks. Modbus is inherently insecure, but very popular in various automation applications. It also provides a very basic data modeling capability. OPC UA can add both security and higher level information modeling capabilities and provide the data from existing Modbus devices to wider area networks, even to the Internet.

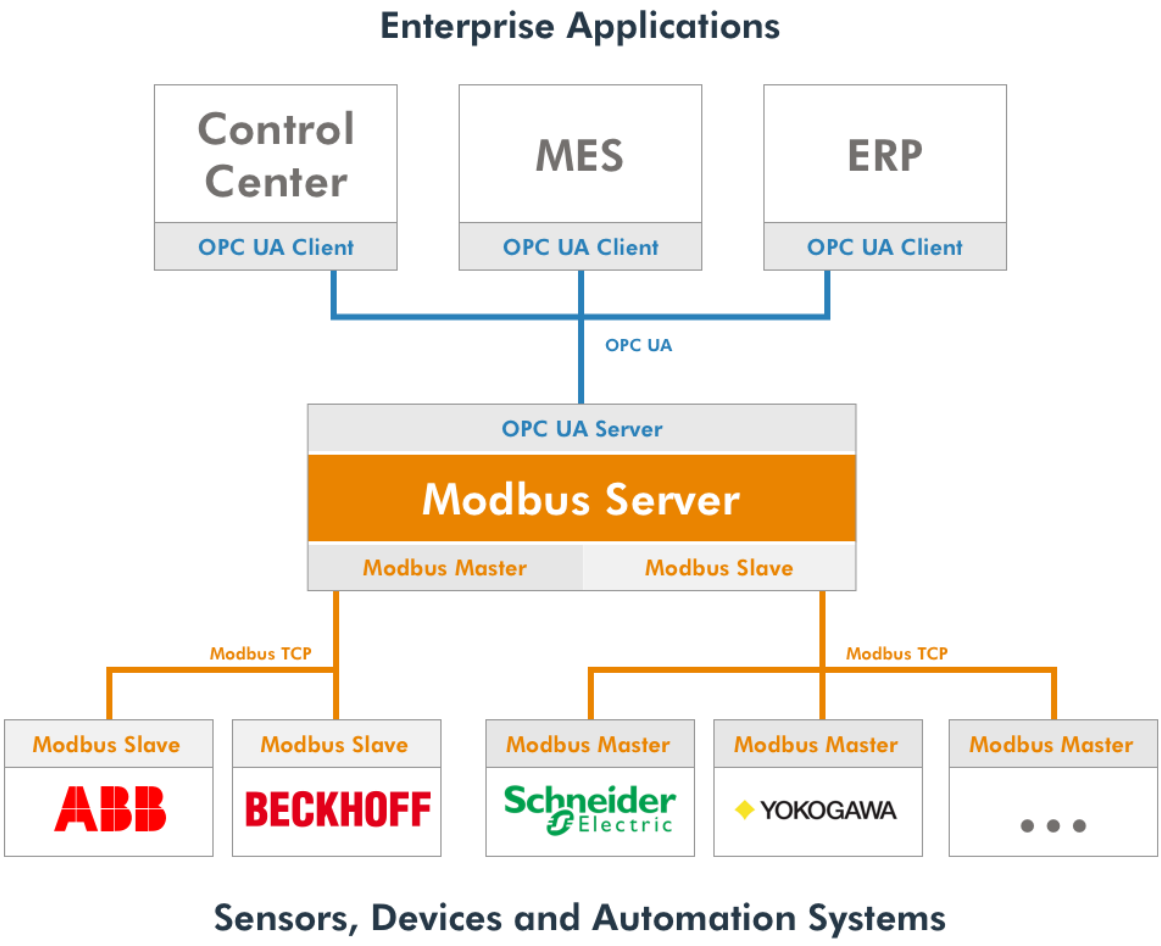

Figure 9. OPC UA Modbus Server acts as a secure OPC UA gateway to Modbus networks.

9 OPC UA HISTORIAN

Another sample application that demonstrates the capabilities of OPC UA is the OPC UA Historian /7/. The application enables "embedding" history to devices and data sources that do not have any long-term history storage capability. Since OPC UA defines access to current values and history from the same source, the product also enables the history to be seamlessly accessed along with the current data, which is passed through the application "as is".

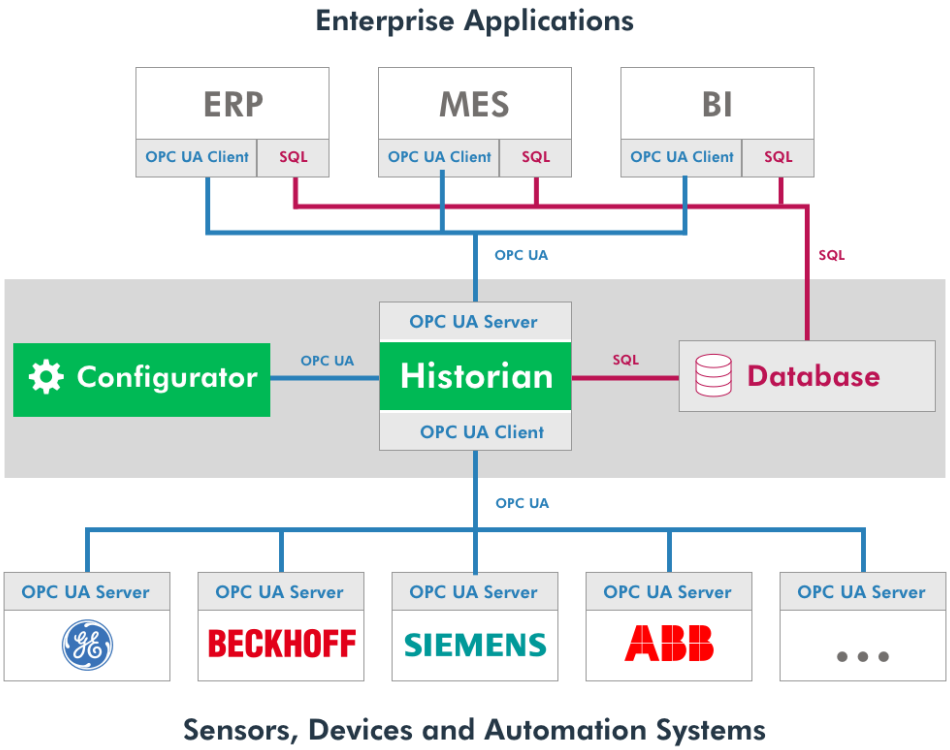

Figure 10. OPC UA Historian adds long-term history for underlying OPC UA servers.

10 REFERENCES

/1/ Plattform Industrie 4.0: *Structure of the Administration Shell*, 2016, https://www.plattform-i40.de/I40/Redaktion/EN/Downloads/Publikation/structure-of-the-administration-shell.pdf

/2/ M.Hankel: *Digitising Manufacturing 2016*, 15.11.2016, http://www.the-mtc.org/Events/Digitising_Manufacturing_2016/4-2_RAMI-Martin-Hankel.pdf

/3/ OPC Foundation:*OPC UA: Interoperability for Industrie 4.0 and the Internet of Things*., 2016 https://opcfoundation.org/wp-content/uploads/2016/05/OPC-UA-Interoperability-For-Industrie4-and-IoT-EN-v5.pdf

/4/ J. Aro, H. Tahvanainen: *OPC UA Enables Secure Data Transfer and System Integrations in Private and Public Networks*, Automaatio XXI seminar 17.-18.3. 2015

/5/ Time-Sensitive Networking Task Group, http://www.ieee802.org/1/pages/tsn.html

/6/ E.Laukkanen: *Java source code generation from OPC UA information models*, Aalto yliopisto, 2013, https://aaltodoc.aalto.fi/handle/123456789/12030

/7/ J.Asikainen*: OPC UA Java History Gateway with Inherent Database Integration*, Aalto yliopisto, 2014, https://aaltodoc.aalto.fi/handle/123456789/13027