Jouni Aro*, Luukas Lusetti, Elias Nykänen

Role-Based Security Management for Industrial Devices and Applications Based on OPC UA

Abstract: Open Platform Communications Unified Architecture (OPC UA, IEC 62541) has become a leading communication framework in industrial automation. OPC UA defines secure communication and information exchange that enable standardized connectivity between industrial applications in process monitoring, production control, manufacturing execution, etc.

In this paper we define a model for centralized security management for all industrial devices and applications, including user management and role-based access control (RBAC).

Keywords: OPC UA, security, RBAC, zones, IT/OT

***Corresponding Author: Jouni Aro:** Prosys OPC Ltd, E-mail: jouni.aro@prosysopc.com

Luukas Lusetti, Elias Nykänen: Prosys OPC Ltd, E-mail: luukas.lusetti@prosysopc.com, elias.nykanen@prosysopc.com

1 Background

Modern manufacturing sites use a varying number of smart devices and applications that are used to control the production on different levels. These applications are installed in different locations and networks within the factory. Some systems are located in IT networks that are connected to the Internet and others in OT networks that are more isolated from the Internet.

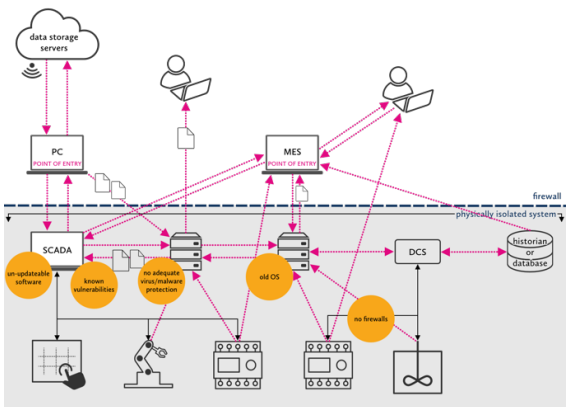

Figure 1. Typical connections across networks in a manufacturing site.

As the production processes get smarter, the IT and OT networks get more tightly connected, since more applications and systems in different networks are installed and they need more connections with each other. As a result, manufacturing networks are typically having many point-to-point connections going across the networks. Over time, this makes it tedious to manage the overall security of the manufacturing site, as shown in Figure 1.

OPC Unified Architecture (OPC UA) [1] enables standard data and information exchange between industrial applications using secure transport level communication [2,3,4].

OPC UA includes high level of security features, including message encryption to ensure confidentiality, integrity and availability of communications. Security is based on reliable authentication, which requires secure management of application and user identities. Authorization can then be applied to different server functionality, based on role-based access control (RBAC) [5].

OPC UA also defines a concept called Global Discovery Server (GDS) [6], which acts as an application registry, but also as a centralized certificate and user management application. OPC UA specification defines how applications can access the services provided by the GDS.

2 Aims

The aim is to present a model for managing application and user identities centrally with optional connections to existing IT network and user management systems via LDAP/AD connections.

The system also enables simple role-based access control (RBAC) based on roles defined in the central management system.

The roles can then be used in the server applications to limit access to critical functionality, such as controlling the devices, or even just to monitor their state.

3 Methods

OPC UA provides all tools necessary to organize secure information exchange between various systems in a manufacturing site. We can use a concept called Aggregation Server to define an application that collects connections to all data sources in a network and provides a single-point-of-access to higher level applications. If this application sits between the OT and IT network, it can also act as a central gate-keeper to all communications between these networks as shown in Figure 2.

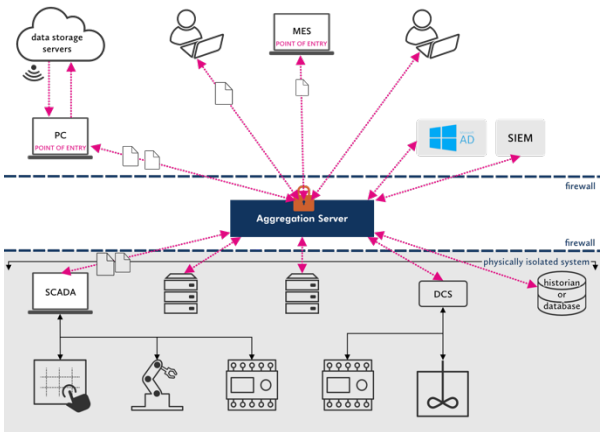

Figure 2. Centralized connections between IT and OT networks.

The Aggregation Server (AS) can include different functionality regarding data and information transformations, but here we concentrate solely on *security controls*. These include:

1. Confidentiality and integrity for data exchange
2. Access control between devices and applications
3. Centralized identity management for applications and users
4. Audit logging of actions

Typically, AS should sit in a De-Militarized Zone (DMZ), which is a separate network between the IT and OT networks, guarded from both sides with a firewall that restricts traffic to the AS only.

In addition to using an AS between the IT and OT networks, a separate AS can be used between all networks boundaries. It can be seen as a context sensitive firewall, even when no DMZ is used between the networks, if the firewall on either side restricts traffic to and from the AS only. ISA/IEC 62443 specifically defines zones and conduits [7] for improved security, and these are in practice implemented with separate networks that are connected to each other with highly restricted firewalls.

In addition to enforcing connections between networks to go via AS, connections between all applications can be enforced to go via AS. In this case, all communication can be monitored and controlled from AS. This can be especially useful, when legacy devices and applications lack specific security features. Using AS in between all communications ensures that all communications will use all necessary security controls.

(1) is applied by enforcing message signing and encryption on all communications, by limiting the available OPC UA Security Modes [2, 4.8] in AS.

(2) is applied by aggregating data and functionality in AS and applying access control measures based on the authenticated applications and users that are accessing specific data and functionality via AS.

(3a) is applied by enforcing all connections via AS and limiting access according to the applications and users identified by AS.

(3b) alternatively, AS can manage the access control lists of the aggregated data sources. This requires that they are OPC UA data sources and that they support this kind of external management as defined in OPC UA specifications [6].

(4) is applied by enforcing all operations via AS, in which case it can also ensure proper audit logging for all communication.

4 Bibliography

[1] OPC 10000-1 (2024). OPC Unified Architecture Specification Part 1: Overview and Concepts v.1.05.04. OPC Foundation.

[2] OPC 10000-2 (2024). OPC Unified Architecture Specification Part 2: Security v.1.05.04. OPC Foundation.

[3] OPC 10000-6 (2024). OPC Unified Architecture Specification Part 6: Mappings v.1.05.04. OPC Foundation.

[4] OPC 10000-14 (2024). OPC Unified Architecture Specification Part 14: PubSub v.1.05.04. OPC Foundation.

[5] OPC 10000-18 (2024). OPC Unified Architecture Specification Part 18: Role-Based Security v.1.05.04. OPC Foundation.

[6] OPC 10000-12 (2024). OPC Unified Architecture Specification Part 12: Discovery and Global Services v.1.05.04. OPC Foundation

[7] ISA/IEC-62443-3-2:2020 Security for Industrial Automation and Control Systems, Part 3-2: Security Risk Assessment for System Design.