Secure and flexible IT-OT integration based on OPC UA

The OPC UA (Unified Architecture) standard has established itself as an enabling technology for ensuring seamless data transfer between these various subsystems, allowing the production (operational technology, OT) and management (information technology, IT) domains to be tightly coupled together.

SOURCE: SOFTING

Middleware can be effectively used to link OT and IT levels flexibly and quickly.

MIDDLEWARE OFFERS THE POSSIBILITY OF seamless and secure data transfer based on OPC UA.

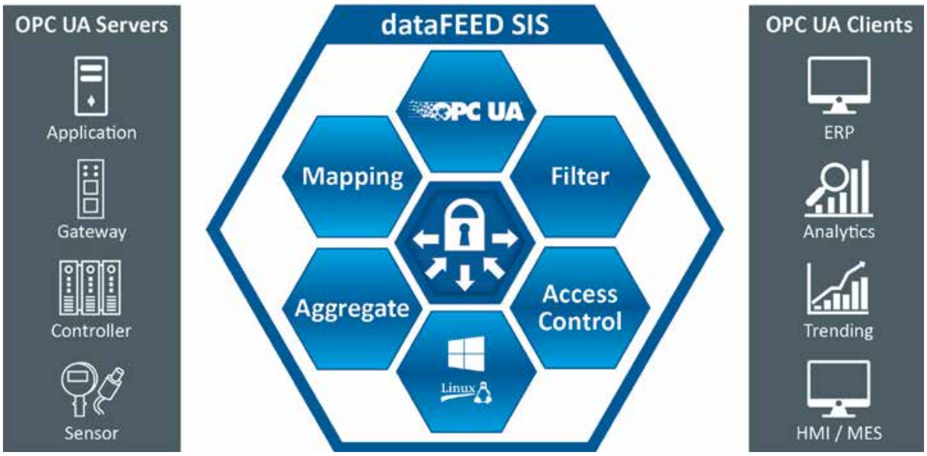
Data transfer plays an especially important role in the integration of the production and management domains, with the large number of variables, heterogeneous interfaces, rights management, and specific security requirements being just some of the key challenges faced in this context. Middleware offers a particularly elegant approach to implementation here.

Driven by factors such as the Industrie 4.0 initiative and concepts like the Industrial Internet of Things, a major trend that can now be seen in production units is the integration of individual components into a coherent overall solution. Increasingly, companies are linking older siloed applications from a wide range of manufacturers with their enterprise resource planning (ERP) and manufacturing execution systems (MES).

Seamless data transfer

The OPC UA (Unified Architecture) standard has now established itself as the enabling technology for ensuring seamless data transfer between these various subsystems, allowing the production (operational technology, OT) and management (information technology, IT) domains to be tightly coupled together. One of the more recent OPC UA extensions, OPC UA Publisher/Subscriber, builds on this by offering an elegant solution for achieving interoperability between control systems.

To handle data exchange within the application as a whole, OT components typically take on the role of OPC UA servers, while IT components play the role of OPC UA clients. Network structure complexity rises exponentially, however, in proportion to the OT and IT applications involved. Data volumes are correspondingly large, and the effort required for installation, setup, and maintenance also increases accordingly. Nor should data security be overlooked in such setups: the automated standalone systems often utilize small OPC UA nanoprofiles that do not support encryption.



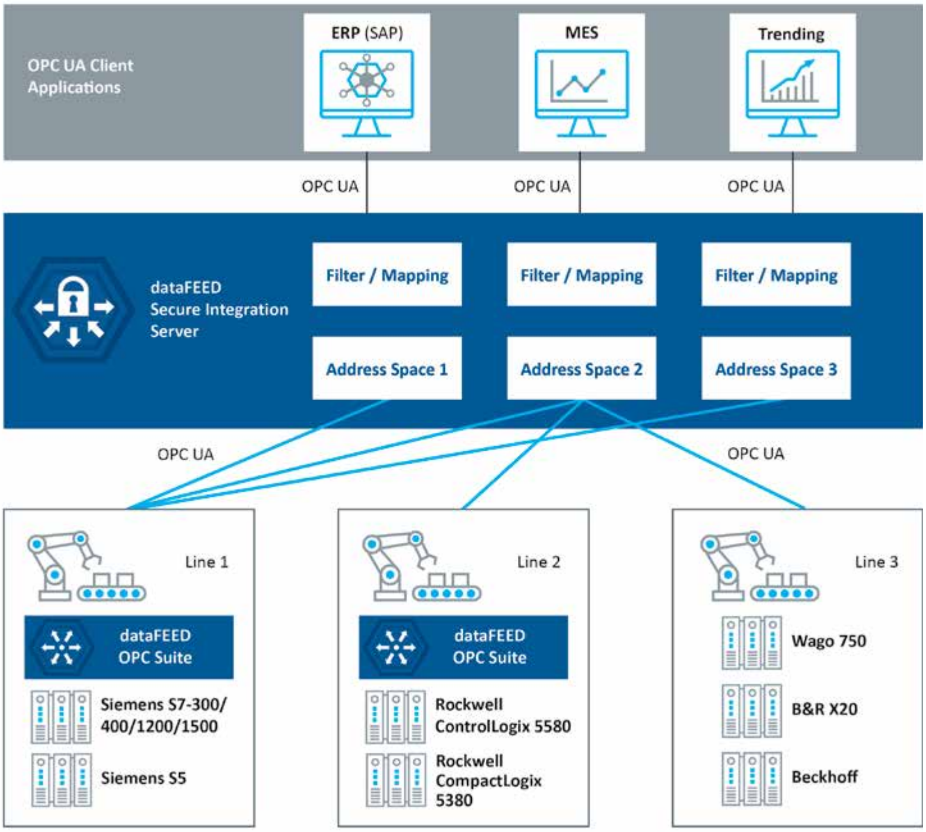
SOURCE: SOFTING

Aggregation server drastically reduces the communication connections in an Industrie 4.0 application.

This is in contrast to the IT systems, for which special security requirements have developed naturally over time, reflecting the fact that these components have to run 24/7. This makes protection from attack of paramount importance, as geographically distant production facilities now need to be connected together around the world and company-to-company networking becomes increasingly desirable.

Middleware: a key component

For the successful implementation of integration applications, these challenges play a central role: to meet them, industry groups like Platform Industrie 4.0 are looking at possible approaches to the optimum solution. The group's position paper 'Secure intercompany communication with OPC UA' (available in German) introduces a number of solution strategies and focuses in particular on the advantages of an aggregating server.



SOURCE: SOFTING

The dataFEED Secure Integration Server meets all of the requirements of a middleware component.

This is the approach taken by the dataFEED Secure Integration Server, a middleware component from Softing Industrial, which provides an abstract interface between the OT and IT domains. Based on the address space modeling defined in the OPC UA standard, the interface utilizes this in particular for interface abstraction and data aggregation.

Interface and data aggregation

Interface abstraction handles changes or extensions within one domain (OT/IT) without any modifications then being required in the other. A user could integrate a new IT application into the overall solution, for example, without needing to make changes to the OPC UA interface at the OT end. Conversely, IT applications do not need to be adjusted to match changes made on the production side, as long as the OPC UA interface implemented in the middleware is kept unmodified.

For software suppliers, this simply involves integrating a standard interface for their application into customer-specific equipment and environments. Users gain considerable flexibility and can exploit short innovation cycles in the IT domain to the full, enjoying an unrestricted choice of the IT applications and platforms to deploy with reduced integration effort. They also benefit from being able to make any changes necessary in the OT domain without having to restart the IT integration process from scratch.

Data aggregation permits data from multiple sources to be consolidated on a single OPC UA server: since IT applications now only need to access this one server, this simplifies and streamlines the underlying communications structures.

This also reduces configuration effort for users, as administrators no longer need to maintain separate sets of configurations for the various IT applications used to access the individual OT data sources. In addition, dataFEED Secure Integration Server also supports the loading of OPC UA Companion Specifications with the information model that these define.

These information models either cover the particular task specifications for a specific industry or define an enterprise object domain. Since this approach also ensures compatibility at the semantic level, users can immediately make use of appropriate objects such as variables or alarms. As one example, the variables defined are all made available with their respective properties such as the unit, the available methods, and services.

Security by design

All of the key mechanisms a comprehensive security model needs for management, policies, and monitoring are consolidated and centralized by dataFEED Secure Integration Server as part of the overall solution. Access rights can therefore be used to control access to individual data items, while applications can also be given their own set of access privileges as well as their own certificates, for example. Filters can be used to further restrict rights. As a result, individual OPC UA client applications can not only limit the entire address space available but can also be required to use the appropriate access service—read, write, browse, or subscribe—to make use of specific data items.

The level of data security provided by dataFEED Secure Integration Server also corresponds to the security functions anchored in the OPC UA standard, which implements Internet security standards as three separate layers. First, user authentication can be handled either by username and password or by digital certificates.

Second, application security can also be achieved by using digital certificates for application authentication. Last but not least, data and messages can be encrypted using the Advanced Encryption Standard (AES) in conjunction with a 128- or 256-bit key. The available security standards are therefore the same as those used for online banking, for example.

To improve security yet further, dataFEED Secure Integration Server also supports the definition of whitelists and blacklists to control data access from specific IP addresses, plus the detection of Denial of Service (DoS) attacks targeting OPC UA authentication.

Benefits for customers

From existing production setups to new installations, choosing to deploy dataFEED Secure Integration Server offers all customers a significant set of advantages when running their applications.

In one recent example, a leading provider of power station process control systems faced the challenge of integrating 1.5 million variables into an overall system. For many OPC UA clients, this volume of variables would be a major stumbling-block. Accordingly, the power station application instead made use of the variable filtering option to restrict access for individual OPC UA clients. To prevent the unauthorized overwriting of assigned values, access to the individual variables configured was also set to read-only.

A major automotive parts supplier likewise chose dataFEED Secure Integration Server to handle the aggregation and filtering of variables from a wide range of heterogeneous OPC UA servers: this enabled access to specific variables from the OPC UA clients over a standard, harmonized interface. Another important reason for this purchase decision was the need to implement state-of-the-art security standards.

Andreas Röck, Product Manager, ***Softing Industrial Automation GmbH.***

Visit Website