EMERSON

news brief

October 25, 2016

Media contact: Grace Capwell
AutomationSolutionsPR@Emerson.com

Emerson technologies overcome IIoT security challenges

Secure First Mile™ architectures maximize operational performance by securely connecting critical operational systems with IT and cloud based applications.

The Industrial IoT presents new opportunities for maximizing operational performance through unparalleled levels of connectivity to analytics and expertise. Getting the right data to the right people can improve plant reliability, efficiency and safety, but with increased connectivity comes increased risk – especially during the "first mile" when data is moved from the plant floor onto the internet to power IT and cloud based applications.

Today's facilities go to great lengths to protect the critical control and safety systems that safely operate their facilities, frequently called "operational technology" or OT systems. Without robust security technologies in place, a plant's assets can be exposed to harmful agents that can cripple operations. When considering Industrial IoT applications that require sensor data in those systems to be transported over the internet, safeguarding against these threats means employing a secure approach for moving sensor data from these sometimes isolated parts of a plant's infrastructure on to the internet without creating vulnerabilities.

Emerson's Secure First Mile™ is a set of architectural approaches and designs, enabled by a family of security services and robust, secure and flexible servers, gateways, and data diodes

that ensures that data in existing OT systems can be easily and securely connected to internet based applications.

This can be accomplished through the more “traditional” Purdue model of network segmentation and firewalls – having data from the most critical OT systems traverse through a number of firewall separated networks, many times passing data through “data aggregation” applications such as historians to provide additional security and access points until it finally reaches a network level that provides controlled internet access. These architectures are found at many larger facilities, and when appropriate IT personnel are available to support them, they are effective. However, they require considerable effort to configure and support correctly, and can require significant effort to add new sensors and make that data available through the multiple layers.

Newer approaches provide connection to OT systems and devices much lower in the architecture, without a lot of intervening software. When devices called data diodes are employed, the biggest concern – that whatever connection has been used becomes an inlet for malicious attacks – can be directly mitigated. These devices physically limit data transmission to one direction – out from the OT systems. Combined with the appropriate protocol translations, simple systems can be constructed that allow highly secure transfer of data from gateways that are talking directly to sensors such Emerson’s 1410 and 1420 *Wireless*HART Gateways.

Using Secure First Mile architectures, a plant can transform its operational technology data into information technology data while ensuring outbound paths of information do not become inbound paths that expose its systems to harm.

Secure First Mile architectures are based on Emerson’s decades of experience creating highly secure control and safety systems and provide support for Industrial IoT enabled devices as well as legacy devices and systems. These architectures leverage Emerson’s existing systems and data collectors, which include distributed control systems such as DeltaV and Ovation, remote terminal units (RTUs) and asset management software such as the AMS Suite. Secure First Mile architectures create secure, direct data export paths from these products and systems to the internet and enable plant personnel to exert tight control over the data that is exported. For example, using software that layers on to the AMS Suite, diagnostic information on a plant’s

equipment can be pre-processed so that only relevant data is exported with the appropriate IoT protocols and security levels.

As part of its Secure First Mile architectures, Emerson is using OPC Unified Architecture (UA) servers to export data from application databases. OPC UA is an industrial machine-to-machine communication protocol that can be directly consumed by Microsoft Azure, Emerson's chosen platform for cloud computing. Microsoft Azure enables the building, deployment and management of applications and services through a global network of Microsoft-managed data centers. Its integrated cloud services include analytics, computing, database, mobile, networking, storage and web applications.

To connect its field data aggregation products such as wireless sensor gateways, CHARM I/O cards, Ethernet I/O cards and RTUs, Emerson is using Windows10 IoT edge gateways. These gateways enable data to securely reach the Microsoft Azure cloud by translating operational technology protocols such as FOUNDATION fieldbus (FF) and HART to information technology protocols such as Advanced Message Queuing Protocol (AMQP) & MQ Telemetry Transport (MQTT). These gateways provide a high degree of security through data encryption and key management. In addition, as described, data diodes installed within the system act as physical barriers to incoming information, preventing outside access to a plant's systems.

Emerson also offers cyber security consulting services to deploy Secure First Mile architectures. Emerson security consultants work with customers' OT and IT departments and their existing security strategies to evaluate existing infrastructure, define the most effective and secure solution to match the business needs for data and applications with the best security architecture to connect to that data. These services are based on decades of securing process critical control and safety systems in applications that range from FDA regulated pharmaceutical facilities to meeting rigorous NERC CIP requirements in nuclear power plants.

Together, these technologies and services bridge the gap between the plant floor and the cloud by enabling secure data collection and aggregation, control over data flow, and the highest standards for encryption and authentication.

About Plantweb

Emerson’s Plantweb™ digital ecosystem is a next-generation industrial IoT portfolio that extends the power of automation beyond process control to the entire enterprise to enable Top Quartile performance. The ecosystem supports Emerson’s Operational Certainty program, which is designed to help companies improve earnings as much as 15 percent. It meets four critical needs to do this: real-time operating data across the business, secure transport of that data where it is needed, robust and scalable software applications to convert that data into actionable insights, and the domain expertise to make decisions and drive outcomes. Flexible, integrated and scalable, the Plantweb digital ecosystem features robust, real-time visibility from Pervasive Sensing™ technologies, protected by Secure First Mile™ connectivity. Applications including Plantweb Insight, Plantweb Advisor and the AMS ARES™ Platform provide embedded domain expertise across the enterprise. Emerson Connected Services offer secure cloud-based access to experts and analytics for real-time asset monitoring and performance optimization with no-to-low capital investment.