control design

WHITE PAPER

Bridging the IT/OT Divide

Today’s smarter edge devices can streamline integration efforts while providing secure remote access for end users and machine builders, too

The Industrial Internet of Things (IIoT) promises a new era of both informed decision-making within the industrial organization as well as data-centric collaboration that reaches beyond the walls of a single factory or even the organization itself.

Achieving this vision requires that system architects and machine designers tap into increasingly powerful—and ever more accessible—information technology (IT) on the one hand while managing a persistent and diverse array of operational technology (OT) on the other. Meanwhile, collaboration across far-flung enterprises as well as with partner and supplier organizations has upped the ante on robust, cybersecure connectivity that often leverages public internet infrastructure.

Facilitating these sorts of capabilities need not be overly complex or prohibitively expensive. Indeed, a new breed of edge devices now are available that feature cybersecure “top-side” integration with supervisory and ERP-level applications—including cloud-based ones—together with “bottom side” industrial protocol integration services for a broad range of controllers and other plant-floor equipment.

Increasingly, this suite of capabilities can be instantiated in a standalone gateway or embedded into another edge device such as a human machine interface (HMI). Further, these newly capable devices can be retrofitted onto an existing machine to streamline enterprise integration or used by original equipment manufacturers (OEMs) to provide out-of-the-box, “IIoT-ready” connectivity on new machines for their end-user customers.

The case for connectivity

While these new edge-device capabilities can advance longstanding objectives of increased visibility in the pursuit of optimized operations, the ability to remotely access a machine's control system also can help to troubleshoot and quickly resolve an estimated 60% to 70% of operating problems, avoiding the need for support personnel to travel across town—or around the world. This applies both to OEMs with far-flung fleets of machines at customer facilities, as well as to end-user manufacturing companies with multiple sites and corporate engineering centers.

The types of problems that can derail production often don't require fixing the machine as much tweaking its programming or other parameters, for example, to accommodate changes in raw materials, machine wear or other production inputs that may have shifted over time. But it's not just the cost of travel that's saved; speedy issue resolution means less downtime and a faster return to full production. And on those occasions when an in-person service call is required, remote visibility can help ensure that the person with the right skills, the right parts and the right tools is sent—increasing the odds of a "fix on first visit" outcome.

The pressures driving industry to adopt remote access strategies have only intensified in recent years as industry faces the continued loss of subject matter experts to retirement. The expertise of those remaining must be stretched over a larger installed base of production machines that is often increasingly global in nature. Further, machine builders are realizing that remote access opens up a new vista of pro-active and preventive services it can bring to bear on behalf of its customers.

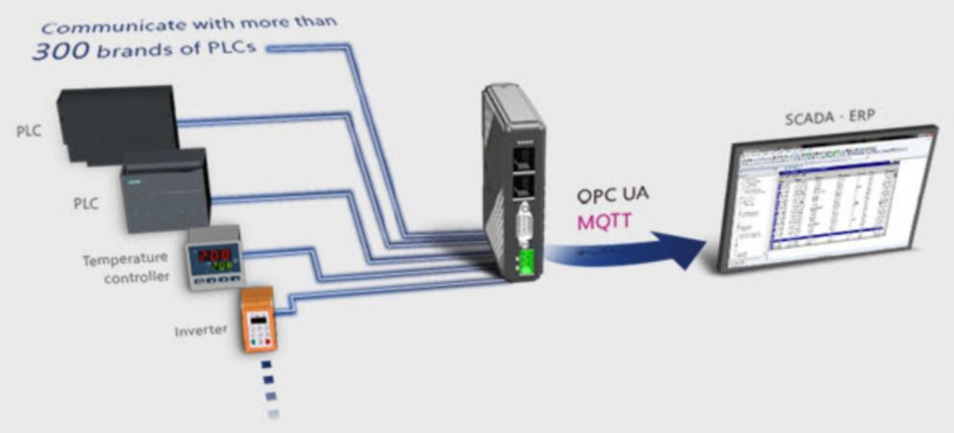

Figure 1. The integration of numerous proprietary plant-floor protocols remains an important function at the interface between OT and IT systems

A foundation of protocol integration

When considering the ability of an edge device to enable remote connectivity and other aspects of IIoT functionality, the connectivity needs of legacy OT technology cannot be neglected. Connectivity to the broad diversity of often proprietary protocols represented by controllers and other plant-floor devices is the bread-and-butter of the industrial human-machine interface (HMI) and industrial PC community, and established players in the space have developed drivers that number in the hundreds. Ethernet as well as RS-232 and RS-485 serial interfaces may be needed depending on the application, and OT device driver support requirements remain as numerous as there are device suppliers in the space (Figure 1).

Other HMI-level functionalities should be considered as well, even if no local HMI display is needed. These include event logging and scheduling, intra-device communication and coordination, as well as arithmetic and logical functions as needed for local data manipulation and analysis.

Standards secure top-side communication

The top-side integration of plant-floor data with supervisory control, ERP and even cloud-based applications is where IT technology has advanced more quickly and is perhaps less familiar to seasoned OT professionals. Here, in addition to familiar Ethernet and internet standards, other messaging and integration approaches such as MQTT and OPC UA have established themselves as key standards.

OPC UA in particular has been codifed by the international community as the IEC 62541 standard, and is specifically cited within the Reference Architecture Model for Industrie 4.0 (RAMI 4.0) as standard protocol for IIoT systems because of its information modelling and platform-independent communication capabilities. And while both OPC UA and MQTT have come to the fore as IIoT enablers, they each have deep roots in the industrial space.

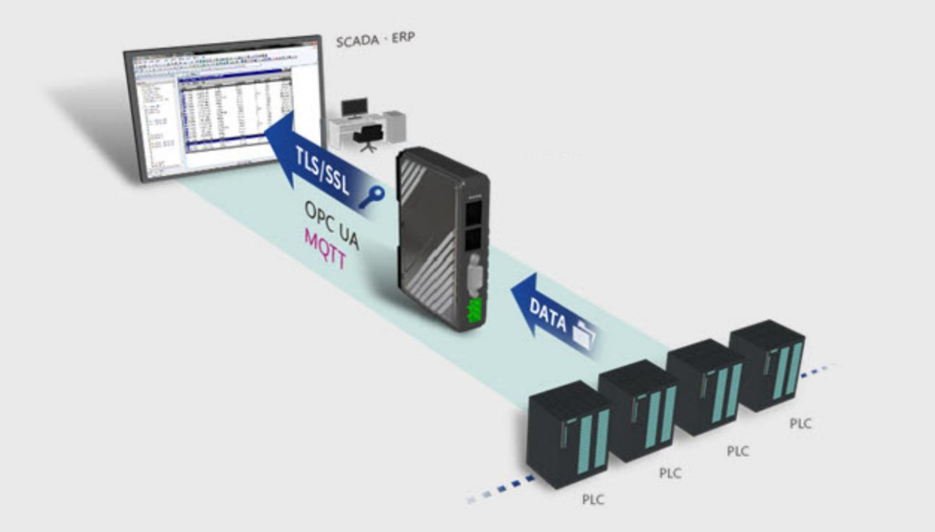

Figure 2. Because both OPC UA and MQTT support TLS/SSL technology for assuring the integrity and confidentiality of communications, they're a good choice for integration efforts that must leverage the public internet to provide connectivity between disparate locations or to partner organizations.

Long before it helped to enable Facebook Messenger, MQTT was developed in the late 1990s for the satellite-based monitoring of oil and gas pipelines. In short, MQTT (which stands for Message Queue Telemetry Transport) is a low-overhead, publish-subscribe messaging protocol that uses a broker to manage the publishing of, and subscription to, communication packets delivered over TCP/IP networks. In the context of an industrial application, edge devices can leverage MQTT to send real-time event/alarm notifications concerning the operation of their machines directly to other machines or to operators' mobile devices.

The original OPC (OLE, or Object Linked and Embedding, for Process Control) standard also dates to the 1990s, when it was developed as an open alternative to the dominant proprietary protocols of the day for connecting programmable logic controllers (PLCs) to Windows-based HMIs. OPC UA (Unified Architecture) has since transcended its early reliance on Microsoft COM and DCOM technology to represent not so much a simple communication protocol but a semantic standard, a framework that allows applications and devices to communicate not just data, but data in context.

Perhaps the most important attribute that MQTT and OPC UA hold in common is the support of Transport Layer Security/Secure Sockets Layer (TLS/SSL) technology for ensuring the confidentiality and integrity of internet traffic by means of a certificate system (Figure 2). This end-to-end encryption methodology guarantees that under no network circumstances will any third party or "man in the middle (MITM)" attacker be able to access the actual data being transferred.

Add to this technology the use of only outgoing, locally initiated virtual private networks (VPNs) to trusted parties for data transfer, and today's edge devices can establish highly secure connectivity to approved applications and subject matter experts within or outside the organization. Some edge devices makers have gone so far as to deploy cloud-based "brokers" that effectively hide and manage all this complexity. Any approved user—with the proper credentials, or course—can have ready access to edge device over the internet without having to remember IP addresses or mess with VPNs. The cloud application securely handles all that complexity on the remote user's behalf.

This white paper was made possible by Weintek, which for more than 20 years has led the industrial marketplace with innovative HMI solutions. The company's latest ground-breaking releases are the cMT-G01 and cMT-G02 smart communications gateways, leading solutions for data transfer and integration into the Industrial Internet of Things.

For more information click here.

WEINTEK