CONTROL

WHITE PAPER

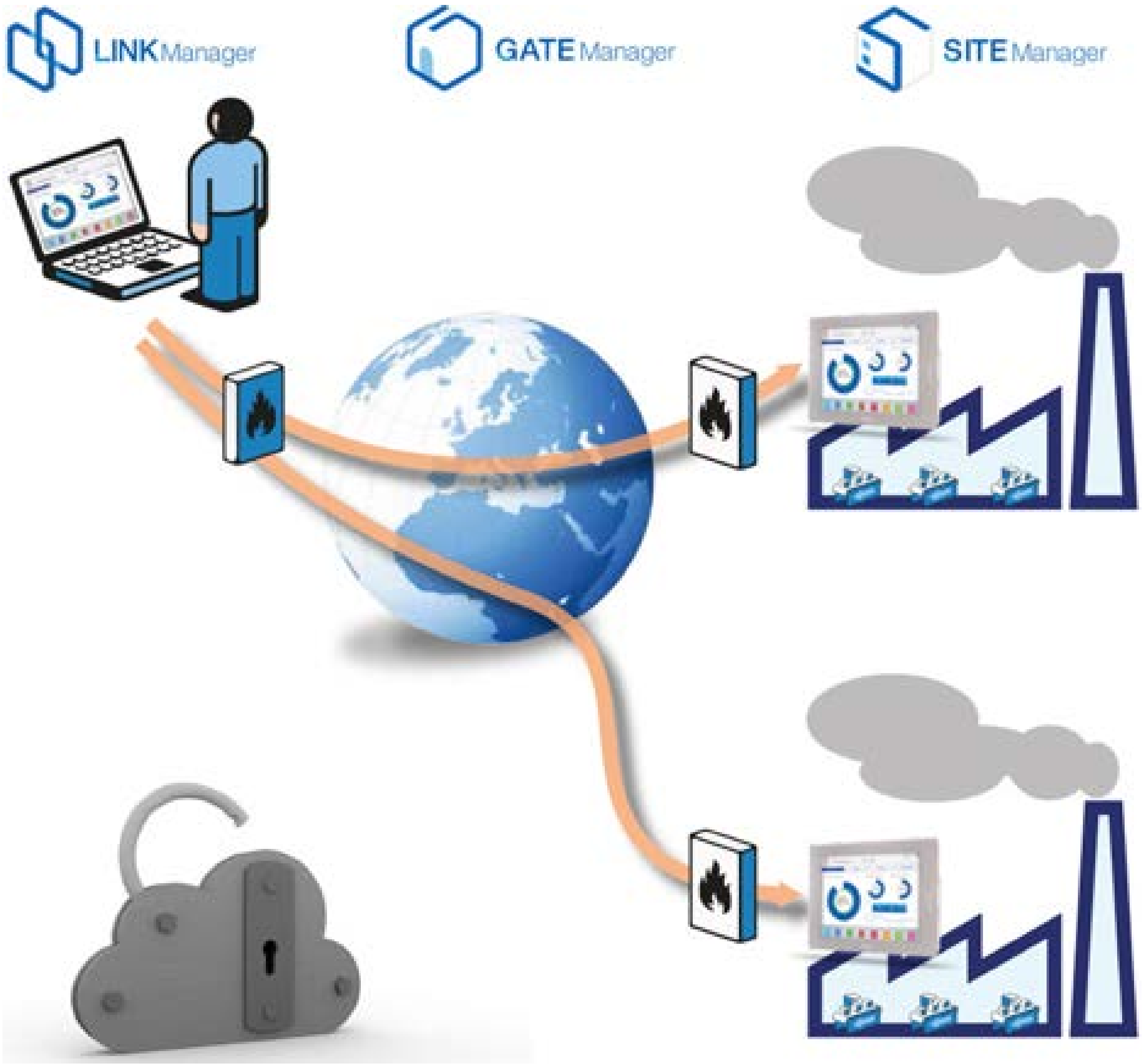
The role of HMI in secure data exchange for cloud applications

How human-machine interface software can provide a layer of protection as well as user-friendly access to plant-floor information

The Russians hacked the grid and shut off the lights in Ukraine, the Israelis used a virus to over-rev and damage nuclear separation centrifuges in Iran, the Chinese—and your competitors—know all your trade secrets. Meanwhile, internet-enabled commercial devices are being hacked and used for nefarious purposes from spying through nanny-cams to empowering denial-of-service attacks. Today, concerns about cybersecurity are a major force damping the free flow of information we need to leverage the cloud and computing power to take advantage of the fourth Industrial Revolution—Industrie 4.0 and the Industrial Internet of Things (IIoT).

Like sergeants on the ground in a war zone, operator- and human-machine interfaces live at the intersection of production and intellectual capital, bringing plant data into IT systems and effecting business information and decisions on often hot, running and critical equipment. Plant-floor professionals are loath to risk compromising production equipment by exposing it to the internet, but are pressured to do so by the competitive advantages offered through access to their operational information.

The conventional approach is to apply security at the information technology (IT) level, but the reputation of IT security infrastructure is mixed, and specialists in operations technology (OT) doubt IT's understanding of OT vulnerabilities. The same problem has become visible in the non-industrial Internet of Things (IoT), and the industrial solution may be to look closer at security technologies coming from the IoT world of connected, commercial devices.



IIoT focusing on security

The IoT world dwarfs the IIoT and is developing its own set of standards, tools and practices to secure everything from aircraft and ATMs to connected cars and global financial transactions. Under constant attack from hackers and criminals of every stripe and subject to the ignorance and mishandling of humanity at large, the IoT is fully capable of developing, testing and proving ways to securely connect the cloud to devices similar to industrial HMIs.

The Industrial Internet Consortium (IIC) recently published “Volume G5: Connectivity Framework” (www.iiconsortium.org/pdf/IIC_PUB_G5_V1.0_PB_20170228.pdf), which provides a reference architecture and outlines the standards necessary for secure and seamless communications. Meanwhile, a lack of consensus standards has not daunted HMI hardware and software companies, which for decades have been providing remote access via the most secure existing technologies. Several have adopted approaches based on Node-RED (https://nodered.org), an open-source development environment invented by Nick O'Leary and Dave Conway-Jones of IBM Emerging Technology Services. In 2016, IBM contributed Node-RED as an open source JS Foundation project, which is now part of the newly launched JS Foundation and recently became a Linux Foundation Project.

Node-RED provides a browser-based flow editor, which can be used to create JavaScript functions. It can be used as a tool for digitally wiring together hardware devices, application program interfaces (API), and online services to provide an easy way to connect edge computing systems such as industrial automation controllers to cloud services such as Amazon Web Services (AWS), IoT, IBM Watson IoT, and Microsoft Azure. It is an open-source technology (available on GitHub.com and npmjs.org), and its development environment can run on platforms including OS X, Microsoft Windows, Linux and Raspberry Pi, as well as cloud services.

By default, the Node-RED editor is not secured—anyone who can access the IP address and port it is running on can access the editor and deploy changes, which is suitable only when it is used on a trusted network. HMI software can secure it by enabling authentication of Editor, Admin API and HTTP interface nodes. Access can then be limited to view-only and restricted to specific nodes, and can be made securely over unsecured Internet or WiFi. By enabling Node-RED authentication and adding user-friendly configuration tools, HMI software vendors can offer a powerful way to securely access industrial equipment.

Industrial-strength Node-RED

For example, Pro-face (a Schneider Electric company) is leveraging Node-RED for industrial HMI applications through Pro-face Connect, which provides secure, remote access over internet (RAOI) for maintenance, control, data collection and monitoring of plant-floor machinery sensors and instrumentation. The software allows users to connect to HMI, PLC, drives and other networked devices like cameras, servers and PC applications from anywhere in the world. No network or firewall configurations are required, and the company says it adds security and encryption "from end to end, from any PC to your machinery," as well as authorization management and access control.

While Pro-face Connect users don’t need to worry about data security and encryption, they do need to make sure they only grant access to machines and devices to authorized staff. Pro-face Connect has a cloud-based “GateManager” where users can specify which machinery can be accessed by whom and from which PC. A “LinkManager” on the user’s PC asks for access permission from the GateManager in the cloud before connecting to a production site and machinery, which improves security because authentication takes place outside of the production facilities. Access can only succeed where “SiteManager” is running on the machinery, which is registered in the cloud-based GateManager for authentication. The SiteManager itself is built-in by standard on Pro-face Smart Portal HMI (Open Box) and doesn’t require configuration. The three--step communication between LinkManager, GateManager and SiteManager allows full control over how selected staff accesses specific machines.

Pro-face Connect users can control or monitor machinery, collect data or perform system maintenance remotely from anywhere in the world through internet with a PC. This allows them to reduce costs by eliminating travelling time and expenses for technical maintenance staff, and shorten production outage time by quick remote intervention on PLCs and drives.

This white paper was made possible by Pro-face America who, for more than 40 years, has set the standard for Human Machine Interface and Industrial Personal Computers. A global company, with a local presence, Pro-face provides global product availability, support, and service. Pro-face helps manufacturers, big and small, solve their toughest factory problems and make their companies efficient, automated and profitable.