APPLIED AUTOMATION

Concept House
Eastern Wood Road
Langage Industrial Estate
Plymouth
Devon
PL7 5ET

FEATURE ARTICLE

Staying secure in a ‘smart’ world

As smart factories become a reality, Applied Automation looks at how companies using remote access communications can protect themselves from cyber attacks using the leading secure remote access solution, Secomea.

Having remote access to machines has become vital for OEMs and system integrators to meet response time and up time obligations. Engineering resources and budgets are limited so efficiency is key. Resolving issues without the need for onsite visits saves time and money but, with the digitisation of factories and enhanced connectivity, come worries over vulnerabilities and IT security. Protecting data when connected to a network can be a complicated challenge.

Applied Automation found an answer with the security certified Danish solution, Secomea. Designed specifically for remote programming, monitoring and data logging, Secomea provides secure remote access without the need for advanced firewall configuration.

Moving on from VPN

Traditional VPN is widely used and suits the job of connecting networks remotely or providing remote access to a central site. However, it has some serious limitations for remote device monitoring and management.

VPN solutions can be complex. Connecting different engineers to different sites around the world by traditional VPN would be a huge task. Setting up a VPN is resource heavy, time consuming and requires the involvement of IT personnel. Subnet conflict issues, firewall setups and single level authentication can also trigger security concerns.

Secomea has developed an internet based technology that specifically addresses the security and usability requirements of linking service engineers with industrial equipment.

Each machine has a SiteManager, a small piece of hardware that the engineer connects to and uses to control the machine. The SiteManager can connect to industrial equipment via LAN, Serial or USB ports. There are also multiple internet access options including LAN, 3G and 4G or WiFi. The LinkManager Windows based client provides (VPN like) access to serial and USB devices, no configuration is required. A web version, the LinkManager Mobile, can be operated from multiple platforms with a browser allowing users to remotely access equipment via a phone or tablet.

The solution also includes a GateManager, a M2M server that is either hosted by Secomea or by the customer themselves. All communication between the factory and the engineer through GateManager is via an encrypted connection. Through the web-based GateManager Portal you can administer accounts, manage SiteManagers and manage devices. It is also straightforward to determine who has access, what equipment and which sites can be accessed and also when and for how long that access remains active. The engineer can securely log on to the system via a X.509 certificate and associated password. GateManager also logs all events.

Secomea has two and three factor security authentication, event audit trails, role-based account management and standard measures for eliminating the risk of vulnerabilities from configuration or human errors.

FLSmidth

This sort of security peace of mind is crucial for FLSmidth, supplier of equipment and services to cement and mineral processing facilities. They remotely retrieve data harvested locally in the PLCs to a central server. The data is then used to create production reports for predictive and preventative maintenance. Data collection is based on FTP access to each PLC via a central GateManager M2M server. After the data analysis, technicians have the option to remotely connect to the monitored PLCs and perform further diagnostics and adjustments.

Future Proofing

Security is the number one priority for Secomea and the company is constantly analysing emerging global security risks. The threats to a company’s data are ever evolving and the need for enhanced methods of securing digital communications will continue to grow with the proliferation of smart, connected factories.

As Industry 4.0 concepts are realised, having future proofed operations and machine control will be vital but they must be secure. Allowing third party access and having different engineers connecting into a factory heightens the security risk.

Secomea has achieved Industry 4.0 certification having proved it enables these connections in a secure way. Unlike an open VPN network, restricting access to certain devices for a specified time is easily achieved using a simple folder and drag and drop system.

The development of smart factories offers significant benefits for the automation industry. If companies are to take full advantage, they must make timely decisions about how to utilise new technology that is designed to keep those connections secure.

Secomea is available in the UK from X-STK | Applied Automation. www.x-stk.com