SECURE FACILITIES

The rise of cyber-attacks means that secure data transmission for industrial facilities is crucial, as **Thomas Holthöfer** explains

Alex/stock.adobe.com

The large variety of machines and plants that has mushroomed over many years is increasingly being networked for monitoring and maintenance purposes. The threat posed by cyber-attacks is highly problematic in the face of old systems and their data connections which lack their own protection mechanisms.

Designed to address this the MICA Edge Computer from Harting, has been designed to enable machines and systems of any kind to be integrated into an Industrial Internet of Things (IIoT) system.

As a result, services such as condition monitoring, predictive maintenance and determining KPIs such as OEE (Overall Equipment Effectiveness) are now possible, not just for new, but for existing plants and equipment as well.

Depending on the application, suitable interfaces and the appropriate software can be combined with the MICA to form a solution package.

When integrating existing systems into a network, besides the availability of plant interfaces, the security of connections and data poses the greatest challenge.

Given this, Harting has developed special protection mechanisms for the MICA mini-computer and enhanced it with security solutions developed in its MICA partner network.

Major cyber risks

A variety of recent studies confirms the growing number of cyber-attacks, and those especially vulnerable are medium-sized production companies. However, according to the VDMA study, "Cyber Risks in Mechanical and Plant Engineering", the majority of companies are not adequately prepared for attacks. The protection that is in place is inadequate and outdated, and consequently there are threats in the form of business interruption and the loss of confidential company data.

"For industrial production security, establish a connection solely to a single machine, rather than immediate access to the entire network."
Josef Waclaw

This is where the MICA and the enhancements developed in the partner network come together.

The MICA has been developed to enable medium-sized businesses, without large IT departments, to securely connect machines and systems.

Protection comprises of five core elements:

- MICA-provided protection due to a secure operating system;
- Protection of applications in the MICA;
- The use of secure protocols;
- End-to-end encrypted data transfer;
- Protection of applications

One MICA network partner is Berlin-based Infotecs, an international IT security provider and specialist in software-based VPN solutions. By combining the MICA with Infotecs' security solutions it is possible to enable the remote control of wind farms, the video transmission of final quality inspection in remote production facilities and the management of remote maintenance access, and early scheduling of maintenance work. With Infotecs' solution, data transmission between the MICA and a remote peer is protected by a bug-proof and tamper-proof VPN connection (Virtual Private Network) and encrypted end-to-end. "The starting point for our security solution is the MICA. The MICA is robust and secure for the industrial environment," said Josef Waclaw, CEO of Infotecs.

Securing the MICA against attacks

The MICA is a mini-computer with network connections. It has a Linux-based operating system and virtualised application environment consisting of Linux containers.

The operating system is designed to be very slim and contains only the software elements required to operate the MICA. This, in itself, helps to eliminate numerous potential attack vectors.

For example, the MICA base system does not include package managers, e-mail clients or other services that are often attacked by hackers. The MICA base system is also inaccessible to users and administrators and cannot be modified by them.

The applications on the MICA also run in separate, virtualised Linux containers. They have been designed so that processes or applications cannot gain access to another container or to the operating system.

While the MICA operating system is provided by Harting, containers can also be developed by third parties, e.g. in order to provide security applications.

End-to-end protection

ViPNet software from Infotecs was developed as a MICA container and acts as a virtual security gateway for the MICA's other application containers.

When the applications send data, the latter are picked up by the ViPNet, encrypted and sent to the equally protected peer. This can be another machine at the same location as well as a remote peer in a remote network, for processing of the process data.

"The protection that is in place is inadequate and outdated, and consequently there are threats in the form of business interruption and the loss of confidential company data."
Thomas Holthöfer

Infotecs CEO Josef Waclaw emphasises that additional safety requirements should be considered in industrial applications. Standard networking applications typically work with web servers vulnerable to cyberattacks. Waclaw cites problems with buffer overflow, insecure protocols and man-in-the-middle attacks.

Consequently, ViPNet software does not use web server technologies. Another difference mentioned by Waclaw is that standard VPN solutions with asymmetric encryption have been developed for office environments. The keys and certificates are first exchanged in the network and a secure connection is then made to the complete network.

"However, for the security of an industrial production environment it's important to establish a connection solely to a single machine, rather than immediate access to the entire network. We achieved this through a direct connection that is symmetrically encrypted end-to-end," Waclaw explained.

The remote peers are also equipped with symmetrical keys, and only those data packets where the key fits are opened. This procedure does away with the necessity of exchanging keys via the network and the subsequent verification of certificates. This is advantageous e.g. for connections via mobile communications, since no additional delays are caused by renewed exchange of keys in the face of more frequent disconnections.

"The solution, in combination with the MICA, protects sensitive equipment and industrial applications. The software is set up once, and no in-depth IT skills are required," Waclaw says.

Author details:
Thomas Holthöfer, Regional Digital Marketing Manager, Harting Deutschland

Security solutions for industrial applications

With the MICA.network, HARTING has set up a user organisation around the MICA Open Computing Platform. A partner network has emerged here that provides solutions for e.g. factory automation, logistics, ERP connectivity, IoT and embedded systems, predictive maintenance and a wide range of security solutions. Berlin-based Infotecs is one of these partners. Perfact and krumedia are among other partners with solutions in the area of data protection.

Remote maintenance solution with central service portal

PerFact:MPA (Meeting Point Architecture) was specifically designed in-house for efficient and controlled collection and troubleshooting malfunctions via remote maintenance. It enables the secure and easy setup of a remote connection to a machine. If a problem occurs on a machine, with the push of a button the customer connects the machine via the internet and the service technician receives temporary access to the machine's controls.

Secure data transmission over public networks

krumedia's SeComBo Suite enables the secure and dynamic networking of individual network subscribers or complete networks via public networks. This is possible even with restrictive security requirements in company-owned infrastructure and data transmission paths. The focus is on ease of use and complete transparency for the devices involved, so that any network subscribers can use these services. Central administration is web-based and requires no additional software.