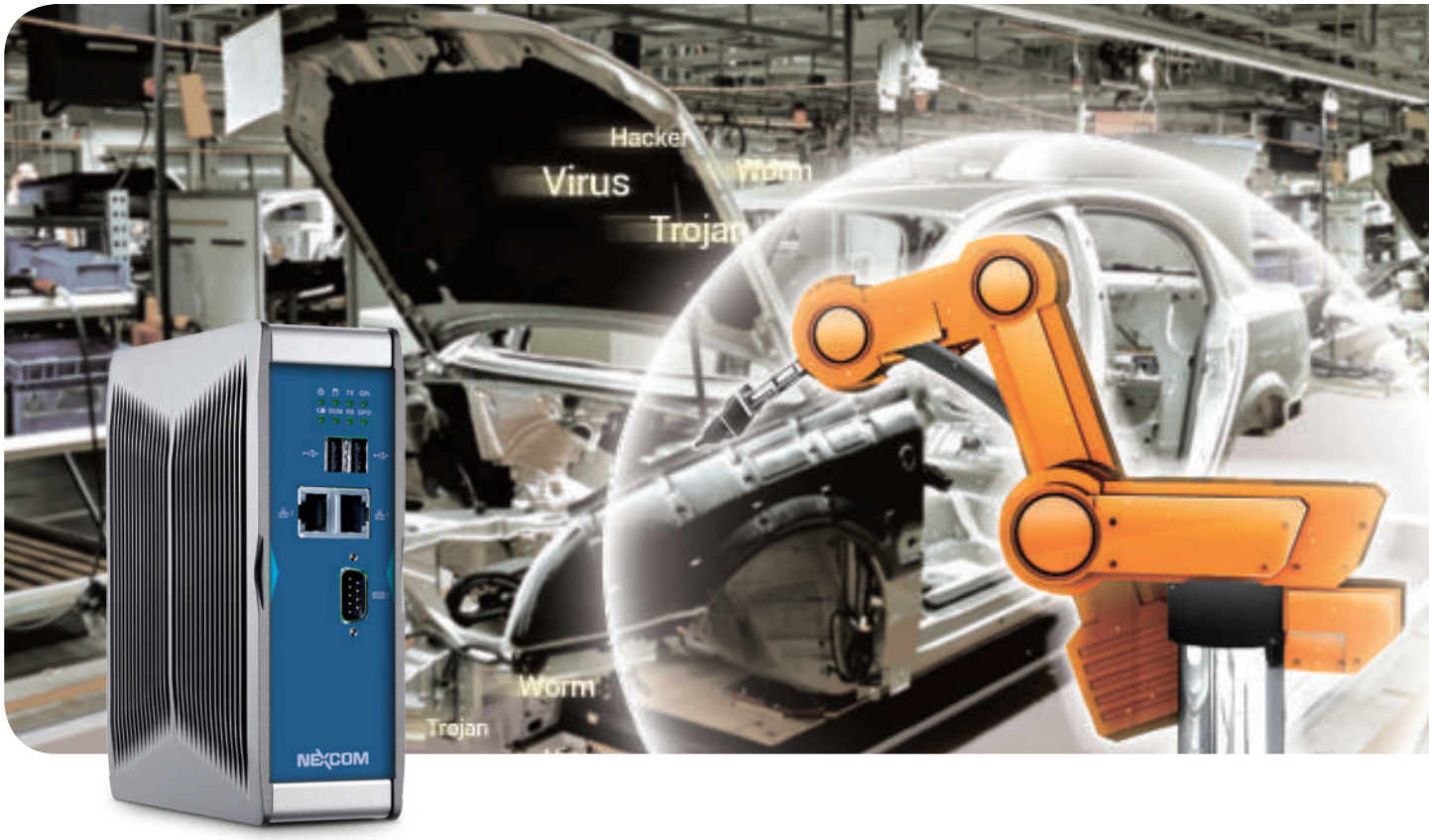

White Paper

Industrial Firewalls Ward Off Cyber Attacks, Keep Industrial Process Control Networks Secure

www.nexcom.com

As industrial automation adopts an Ethernet-based network, production processes in factories can achieve intelligent manufacturing and benefit from real-time monitoring and remote management. However, these benefits also introduce new security loopholes for industrial process control networks, increasing their vulnerability against cyber attacks. Therefore, establishing a protection mechanism for industrial process control networks has become imperative.

In the past, industrial process control networks used proprietary protocols and were isolated from the public network. The advent of intelligent manufacturing, along with the proliferation and cost reduction of Ethernet and networking, industrial process control networks are gradually converging to Ethernet-based open networks. However, once industrial process control networks are exposed to the public network, security loopholes may be exploited. To prevent production lines from malicious interference, industrial process control networks require protection by industrial firewalls.

Safeguard Industrial Process Control Networks with Deep Packet Inspection

"Although commercial firewall technology has advanced significantly and received widespread adoption throughout the years, they are not designed to protect industrial process control networks. Due to the application differences between a commercial and industrial process control network, it requires an industrial firewall to secure sensitive and critical data exchanged in industrial process control networks and provide a deeper level of management and protection of nodes," explained Hadwin Liu, director of product management, NEXCOM's Network and Communication Solutions Business Unit.

Liu further explains that the enterprise network is made up of three layers, which are intranet, plant network and industrial process control network, or process control network for short. Industrial firewalls' main purpose is to protect the industrial process control network, which monitors and controls all the internal nodes and ensures that all the nodes are functioning in optimal condition. Although the network bandwidth at this level is not excessively demanding, the transmitted data is highly valuable, such as monitoring variables used to assess the level of alkalinity in wastewater treatment plants, or control variables used to control industrial robots in factories. Therefore, industrial firewalls need to support various Fieldbus protocols such as PROFINET, as well as provide deep packet inspection in order to inspect and analyse the header and payload encapsulated at different layers of the packet to ensure integrity.

In contrast, commercial firewalls do not support Fieldbus protocols and they focus on inspecting packets that are based on common communication protocols such as email, file transfer and web browsing, making them unsuitable for industrial process control networks.

For example, at an automotive assembly line, the industrial robots function as network nodes that operate according to the control command received. If the packets sent to them contain suspicious instructions, such as instructing the industrial robots to perform actions that are not part of the standard operating procedures, the automotive manufacturer may suffer huge financial losses due to the mass production of inferior products caused by compromised nodes. By incorporating industrial firewalls, any suspicious packets can be identified and blocked, preventing the control command from being tampered with and ensuring the industrial robots are operating as programmed at all times.

The security of industrial process control

networks is strictly managed due to the specialized nature of the production nodes. Since these nodes only execute a limited set of applications, industrial firewalls use a whitelist to specify which applications can traverse in and out of the network, while blocking all others. Commercial firewalls, on the other hand, use a blacklist to provide security at the entry point of the company's network, and will only block applications specified in the list. Hence, industrial firewalls are more effective at protecting industrial process control networks.

In addition to a whitelist, virtual private network (VPN) is also another important feature for industrial firewalls. As industrial process control networks are converging to Ethernet, information will be exchanged in an open network environment. To ensure the information received from a remote site is complete and authentic, VPN will create a private channel on the public network and encrypt all the information within, even if the data is eavesdropped during transmission, the data will be difficult to decrypt and tamper with.

Delivering Uninterrupted Production in Harsh Environments

There exists a diverse range of industrial automation applications, such as oil fields in hot deserts, steel plants that are exposed to scorching heat and wind farms in salt fog environments. To withstand these extremities, industrial firewalls require a rigid and robust design to maintain reliable operation under high temperature, high humidity and high salt environments. Moreover, a heavy emphasis on stability with low or no downtime is required from each production node especially during critical production processes. Thus, industrial firewalls must provide high availability by featuring redundant mechanism that can resume operation within a short amount of time to provide constant protection of the industrial process control network.

Using Ethernet, intelligent factories are able to monitor and manage the entire plant operation from a remote location in real time. From a managerial point of view, Ethernet-based intelligent factory is a valuable asset to improving a business' manufacturing and management efficiencies. However, from a security point of view, any security breaches cannot be tolerated. Ever since the cyber attack on Iran's nuclear power plant in 2010, industrial users have realized the importance of industrial process control network security. In the quest of protecting the value of production nodes, industrial firewalls are recognized as the key solution. With great development potential, the future of industrial firewalls is bright ahead.

About NEXCOM

Founded in 1992, NEXCOM has five business units which focus on vertical markets across industrial computer, in-vehicle computer, multimedia, network and communication, and intelligent digital security industries. NEXCOM serves its customers worldwide through its subsidiaries in seven major industrial countries. NEXCOM gains stronghold in vertical markets with its industry-leading products including the rugged fanless computer NISE series, the in-vehicle computer VTC series, the network and security appliance NSA series and the digital signage player NDiS series. www.nexcom.com