Category A

IT Security and Safety for Automation, Cyber Security

GIT SECURITY AWARD 2021 FINALISTS

ABB Stotz Kontakt: HD5

Three-stage Enabling Device

The new three-stage HD5 Enabling Device offers maximum safety with extraordinary flexibility and perfect ergonomics. The optional emergency stop, the integrated flashlight and a motion sensor provide additional functions and optimum safety for the operator. Freely programmable control and signal elements for visual and haptic feedback allow for individual and customized use. Furthermore, the housing complies with the guidelines of "hygienic design" and is made of the highest quality materials. This ensures functionality also in demanding application environments. HD5 complies with protection class IP65 and has received CE, TÜV-Süd and cULus approvals.

AIT Solutions: Herakles

Network Management Systems

The Herakles network management system covers three basic areas in the OT environment: asset management, configuration monitoring and documentation of known errors. These elements are the basis for the implementation of security measures. While these use cases have long been solved in IT-based devices, a corresponding simple solution for OT devices has been missing until now. Herakles now closes this gap by detecting and monitoring all Profinet components including firmware or hardware states as well as all basic configuration properties – device name, IP configuration or topological relationships. If changes occur, the users are informed accordingly. Herakles thus creates a fundamental basis for cybersecurity strategies in the OT environment of manufacturing companies.

Bihl+Wiedemann: ASi-5

Feldbus Gateway

ASi-5, the evolution of the proven standard AS-Interface, stands for great data bandwidth and short cycle times. In this way, larger amounts of data can now be transferred much faster. In addition, the integration of intelligent sensors and actuators such as IO-Link is now considerably easier, with simultaneous downward compatibility to all previous ASi generations. Since energy and data are transmitted simultaneously on the yellow ASi cable, the cost and wiring effort is much lower than with other fieldbus systems. Last but not least, the onboard web server enables a simple diagnosis & remote maintenance, whereas the integrated OPC-UA server allows simple incorporation into Industry 4.0 applications.

Claroty: Continuous Threat Detection (CTD)

OT Security Platform

CTD bridges the IT/OT security gap. It automatically discovers OT systems and IoT devices on the network and classifies each device based on both static and behavioral attributes. CTD thus enables complete visibility into OT networks, the ability to discover and manage all assets within those networks, and continuous monitoring of all directly relevant threats and vulnerabilities. CTD leverages Claroty's proprietary deep packet inspection (DPI) technology to extract precise details about each asset on the OT network, profile all communications and protocols, generate a fine-grain behavioral baseline that characterizes legitimate traffic, and send real-time alerts on baseline deviations, as well as the presence of indicators of compromise (IoCs) and exact-match vulnerabilities within your environment.

Euchner: CTM

Transponder-Coded Guard Locking Device

The new transponder-coded CTM guard locking device has been specially developed for use on small flaps and lightweight doors on packaging machines and is particularly impressive due to its small dimensions. It is one of the smallest guard locking devices on the worldwide market and provides process and personnel protection in the smallest of spaces. The guard locking device can be integrated almost invisibly into machines, providing design engineers with greater freedom. Despite its compact design, the CTM has a locking force of 1000 N and offers reliable safety door protection in accordance with Cat. 4/PL e as per EN ISO 13849-1 (highest protection class IP69). The CTM is also available as a hygienic variant and offers future-proofing in terms of Industry 4.0 thanks to intelligent communication capabilities.

Georg Schlegel: Emergency Stop Series Test Machine

Fully Automatic Test System

In case of an emergency, emergency-stops are crucial. Thus, quality has top priority for manufacturers. To be able to completely cover every safety-relevant parameters, the company Georg Schlegel has designed a fully automated test system. For 225 variants the robot is measuring the threads, the forcedistance ratio and the torque, a visual inspection is done simultaneously by cameras. By means of the serial number, which the robot prints on automatically and the inspection record the result´s traceability is always guaranteed. In cooperation with all departments involved the requirements for the testing system were documented in a specification sheet.

KEB Automation: Combivert F6 Pro

Drive Controller with Encoderless Safety Functions

The Drive Controller Combivert F6 from KEB Automation is frequency inverter and servo drive in one device. It is applicable for control of different motor technologies with or without encoder. The safe operation of machines often requires safety functions to limit speeds, directions or axis positions. The Combivert F6 offers scalable safety functions directly in the drive and in the new device variant Pro also many functions without external encoder – unlike previous solutions with classic, safe encoder feedback. In this way, safe solutions can be implemented, for example, in applications in which no encoder signal is possible. Encoderless safety functions offer cost-efficient options for simple motion monitoring in addition to more individual machine concepts.

MB Connect Line: mbNetfix

Industrial Firewall

Controls and other components of production plants often have no security functionality of their own. In order to enable secure networking, it is recommended to segment the production network and only allow defined communication at the junctions. The self-learning industrial firewall mbNetfix is ideally convenient for this. Using a whitelist, the user defines which connections, services and protocols are permitted. Any other communication is blocked. To control the communication traffic, the firewall can filter out the allowed and forbidden traffic based on the source MAC/IP addresses, the destination MAC/IP addresses and the ports. In order to keep the attack vectors as small as possible, mbNetfix was designed without a web interface already during the development of mbNetfix.

Moxa Europe: Intrusion Prevention System (IPS)

Cyber Security Solution for OT and IT

In order to ensure that network activity on industrial networks is authorized, Moxa's industrial cybersecurity solution allows to define granular access controls at different levels. One can define a whitelist of devices and IP ports that are allowed to access all or part of the entire network. In addition, one can also define the authorized protocol format to prevent unauthorized commands from passing through the industrial IPS or firewalls. Furthermore, OT engineers can even define which control commands can pass through the network to reduce human error associated with sending a wrong control command. In addition, the IPS provides virtual patching of vulnerabilities for operating systems, application software, and industrial equipment such as PLCs.