Cyber security for automation

ABB showcases its latest comprehensive services, such as life cycle management and cyber security, for ensuring secure operation of IT structures in production.

IT security services
Cyber security is becoming an increasingly important issue in process automation and particularly for process control engineering. As networking in process automation grows, there is a greater risk of cyber attacks from different channels. This could have a massive impact on management and control systems, with the potential effects ranging from production failure, pollution, personal injuries and damage to a company’s image, to the loss of confidential data. ABB offers advice and services specifically to combat these threats. Together with our customers, we develop security plans that meet the individual requirements of each production environment. This may involve a single automation system or multiple systems with central security management.

Cyber Security Monitoring Service
ABB’s Cyber Security Monitoring Service identifies, classifies and prioritises possibilities for improving control system security. It monitors the security standard set and compares captured data against best practices and industry standards in order to identify any potential weaknesses in the system. The Cyber Security Monitoring Service is accessed via ABB ServicePort, a remote service provision platform. It enables users to call on ABB’s services and experts securely to meet their specific requirements and can be integrated into the company’s existing control system. As a result, users can view data recorded and stored via the web-based ServicePort channel that can be accessed easily by customers or ABB personnel. Users gain a scheduled or responsive security monitoring service, including data analysis.

Security Update Service: patch management and malware protection for process control systems
The Security Update Service provides Microsoft security patches and McAfee and Symantec virus signatures, which ABB has tested and approved in its own security laboratory to ensure compatibility with ABB control system software. These tools can be downloaded from the ServicePort platform via secure remote access and imported into ABB control systems. Timely updates guarantee maximum protection against attacks on the system. We offer daily virus signature updates. If required, an email alert can be issued if a virus is discovered or a virus signature update fails. If you wish, the Microsoft security patches can be activated locally by ABB, by rebooting the nodes in a defined cycle while taking into account the availability requirements of your plant. Because the data transfer is performed entirely via an SSL-encrypted remote connection, it guarantees secure, straightforward access and smooth integration into the plant operator’s IT structure.

When cyber security plans are worked out and implemented, the availability of control and automation systems is just as high a priority as ensuring adequate protection for the company and minimizing the risk of cyber attacks across the company. ABB has developed the Cyber Security Fingerprint to this end. This is a non-invasive service that can be used on most control systems with the latest versions of Microsoft Windows. By applying data collection methods, industry standards, best practices, robust technology and system security expertise, it helps companies to protect valuable resources.
Customer portal displays system documentation over the control system's entire life cycle

The new, secure myABB/My Control System customer portal is available 24/7 and gives plant operators a central access point to information relating to the installed ABB control system as well as other ABB products. A modern navigation concept that is also designed for use with mobile devices makes it easy to get fast access to detailed information about the software, the system status, reports, alerts, online tutorials and service contact data right through to system documentation.

A dashboard in the customer portal provides customised access to security reports, product alerts and documentation relevant to the installed control system, and displays key information on the subscription and software licences specific to the control system in the form of content, expiry dates, tool downloads and licence key downloads. All of this data can be called up with just a few clicks and the support jobs such as software licence management, updated protection against malware are facilitated.

Thanks to innovative data management, users are in a much better position to plan, optimise and continuously improve plant processes, which in turn strengthens competitiveness in a fast-paced market.

Increasingly, control system users are devoting greater attention to cyber security and are planning measures to protect the availability, integrity and confidentiality of their systems. ABB offers an extensive range of services that are continuously being updated and enable plant operators to raise the security of their IT systems to the highest possible level. The costs caused by cyber crime are much higher than the costs of measures to protect against it.

About ABB

In 2016, ABB Germany generated sales of EUR 3.28 billion with 10,540 employees. ABB (ABBN: SIX Swiss Ex) is a pioneering technology leader in electrification products, robotics and motion, industrial automation and power grids, serving customers in utilities, industry and transport & infrastructure globally. Continuing more than a 125-year history of innovation, ABB today is writing the future of industrial digitalization and driving the Energy and Fourth Industrial Revolutions. ABB operates in more than 100 countries with about 132,000 employees. www.abb.de

For further information please contact:

Media Relations
Rainer Hofmann
Tel.: +49 69 7030 4308
E-Mail: rainer.r.hofmann@de.abb.com