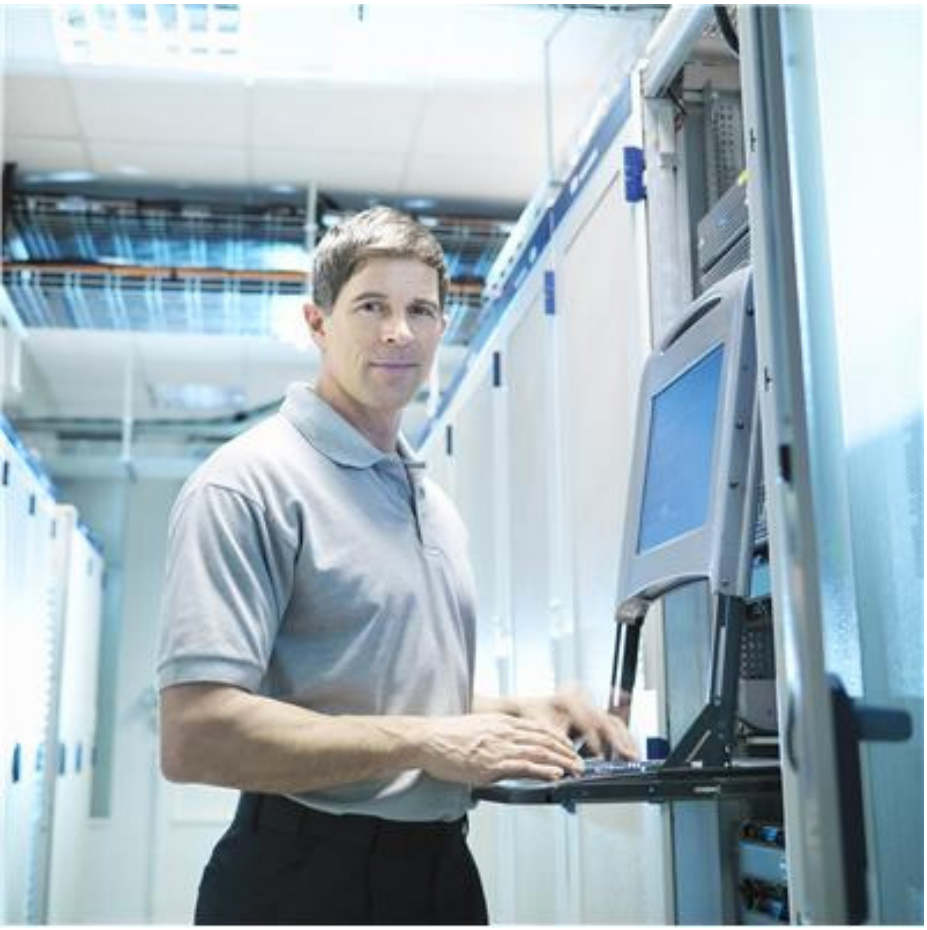
EXECUTIVE REPORT

Resilience for process control systems
Cyber Security



01 Cyber-attacks on process control systems can have more serious consequences than those on commercial IT. IT departments must therefore develop an understanding of the requirements for the protection of IACS networks.

The costs of cyber-attacks are around two to three times higher than the costs for appropriate security provisions – at least! There are a number of issues with process control systems, in particular if these are not in isolated operation but are networked with supplier IT.

Cyber-attacks have already led to security breaches at large companies and even government organizations. The increasing networking and growing criminal energy of the hackers are making IT systems of all kinds more and more susceptible to this. Until recently, industrial systems that monitor and control production processes, the classic automation systems, had remained relatively untouched by this. The online threat to process control systems is greater today than ever. Cloud computing and the increased abilities of hackers are constantly worsening the situation. While corporate IT had been the preferred target of hackers until now, they have now begun increasingly to turn their attention to automation systems in production. The increasing distribution of process control systems in newly industrializing countries in which security consciousness is not yet as widespread further aggravates the problem, the experts warn.

Previously, the process control systems in a plant were isolated from the other information systems. Now increasing economic pressure demands an integrated approach. Internally, utilities companies and industrial companies are increasingly relying on the exchange of relevant data to receive more detailed insights into operation. In addition, process control systems are extremely long-lived, with a lifecycle of 15 to 20 years. For this reason, relevant protective measures against online attacks are either not up to date or are even not available at all, or else people simply rely on the measures taken by corporate IT. Furthermore, many systems contain smaller, subordinated software packages that are not designed to execute anti-virus software or firewall programs.

As the threat through improper handling of storage media and through cyber-attacks has increased significantly over the past 10 years, governments and companies find themselves compelled to work together to prepare themselves for such attacks and to limit the economic risks that these bring with them.

Partner for cyber resilience

The World Economic Forum recently started an initiative with the name Partnering for Cyber Resilience to strengthen the ability to withstand cyber-attacks. This obligates signatories to recognize the significance of working together, to develop risk management programs and to encourage partners and suppliers to likewise commit themselves to the fight for security on the Internet. While governments and company managers recognize the situation, the top and middle management and the system administrators at many companies have often not yet recognized the seriousness of the situation. It is important to strengthen the resistance against cyber-attacks by means of joint efforts with the producers of industrial IT technology.

One thing should be clear here: 100 percent security against cyber-attacks cannot be reached, even if a system is equipped with the most up-to-date security measures. The constantly increasing number of less secured connections to suppliers', contractors' and partners' networks remain vulnerable. Many industrial managers are still of the opinion that this only applies to company-wide IT systems like computers, servers and other network facilities. Frequently people forget that, with the spread of industrial technologies, additional dangers arise through connections to supplier networks, such as remote maintenance facilities. This means that the security requirements need to be considered in the same way. Even isolated IACS systems (industrial automation and control systems) that only have minimal exchanges with external suppliers, producers or partners are endangered by attacks through PCs, storage media, the unauthorized installation of software or even targeted attacks by the company's own employees.

The ABB Ability™ Cyber Security Monitoring Service identifies, classifies and prioritizes possibilities for improving the security of the process control system. It monitors the Internet security and compares the recorded data with best practices and industry standards in order to reveal vulnerabilities. Access to the ABB Cyber Security Monitoring Service is via the ABB ServicePort, a remote-based platform for providing services.

It provides individual, secure integration of ABB services and experts and can be incorporated into any process control system. With this, users can view data that is recorded and saved via a web-based channel in the ServicePort that can easily be accessed by customers or ABB personnel. The user receives scheduled or requirements-oriented security monitoring including data analysis.

Cyber security is an integral component of ABB's products and systems and is taken into account in every phase, from design and development to maintenance and support. This includes threat modeling and security design reviews, security training for software developers and the internal and external performance of security audits as part of quality assurance.

Examples of improvements in cyber security can be found in the latest release of the ABB Ability™ System 800xA, which includes extensive functions for the most secure possible operation of process automation solutions. This includes support for solutions to protect against malware from third-party providers (anti-virus programs and positive lists for specific applications), granular access control (flexible account management as well as granular access rights and role-based access control) and secure communication by means of IPSec (Internet Protocol Security). However, the security aspects are not limited to system functionalities, but also include support during the product lifecycle, for example through validation of security updates from third-party providers and a standardized process for dealing with weak points (vulnerability handling).

When it comes to company-wide IT systems, in the event of a cyber-attack the protection of confidential data must be top priority, followed by the integrity of the system and finally the availability of information for authorized network users. However, when using this strategy for a cyber-attack against an IACS network, the priorities are entirely different.

Here, the risk focus is on availability, closely followed by integrity; the confidentiality of information is of lesser importance.

—
02 The 800xA automation system includes solutions for protection against malware, granular access control and secure communication via IPSec.

Corporate IT and process control system IT function differently

How companies react to a cyber-attack depends on who is responsible for corporate IT and who for process-system IT. For the corporate IT department, the criticality focus is on the resilience of corporate IT. The departments responsible for process control system IT are responsible for the safe and uninterrupted running of the production process and, due to the traditionally isolated character of such IACS networks, have little experience with the topic of cyber security. As a result, the process control IT is more susceptible to cyber-attacks, the management of which is the responsibility of corporate IT, who frequently do not understand the diversity of the IACS networks and their complexity. For this reason, the two areas need to build bridges so that IACS engineers and IT specialists speak the same language and recognize that IACS networks are susceptible to cyber-attacks, but that not all security measures that apply to the company network can simply be transferred.

When developing and implementing plans for cyber security, sufficient protection of the company and company-wide risk minimization in the event of cyber-attacks must ranked equally with the availability of process control and automation systems. ABB has developed the Cyber Security Fingerprint for this purpose. This is a non-invasive service that can be applied to most process control systems with current versions of Microsoft Windows. It helps companies to protect valuable production facilities through the use of data collection, industry standards, best practices, robust technology and system security expertise. With knowledge regarding the security deficits of process control systems, industrial companies can create plans that:

- Increase the protection of plants and the community
- Reduce the danger of system and plant faults
- Reduce the risk of an online attack
- Lower the costs for detecting and fighting cyber criminality
- Supply a solid foundation for establishing a sustainable cyber security strategy

Process control system users and plant managers should therefore increasingly turn their attention towards cyber security and plan measures to protect the availability, integrity and confidentiality of their systems. The costs caused by cyber criminality are at least two to three times greater than those for appropriate protective measures. Investments in cyber security thus also make sense from a financial standpoint. Similar to process and safety improvements, cyber and IT security improvement needs to be a continuous activity. Correct management and regular cyber security assessments are key to ensuring a consistent security level of the process control system across the entire lifecycle.

—
ABB Inc.
579 Executive Campus Drive
Westerville, OH 43082 USA
automation.service@us.abb.com

abb.com/cybersecurity

9AKK107198