Situation and requirements in the market
Nowadays, the number of targeted cyber attacks is constantly increasing against plants or control systems. To avoid such cyber security attacks, critical infrastructures require accurate compliance with IT security policies. The problem is often due to insufficient knowledge about the safety condition of the system, which is why the right measures are difficult to select.

In addition operators have excellent knowledge of the operation of the system, but not in cyber security. What is important for cyber security is the obligation to implement the prescribed catalogue of measures, as well as a continuity of monitoring and appropriate measures. By implementing the measures customers can achieve an increased plant availability.

The future of cyber security of process control systems is comparable to the information technology in the company. With cyber security services, our customers enjoy continuous high-quality cyber security monitoring. ABB offers its customers proactive action with short response times for possible cyber security incidents. All actions are supported by extensive expert knowledge from the Collaborative Operations Center.
The new ABB Ability™ Collaborative Operations Centers offer cyber security solutions for our customers' control systems. ABB provides high-quality support for optimizing productivity and lifecycle costs based on extensive global experience with similar systems.

**Customer value:**
- Compliance with individual and legal requirements
- Continuous monitoring, proactive actions
- Improvement and maintenance of cyber security over the entire lifecycle of the system
- Higher availability of the plant
- The minimization of the risk of data loss from potential cyber attacks
- Faster access to expert knowledge

**Our solution:**
- Cross-industry expertise from the Collaborative Operations Center
- Operating a security patch management infrastructure
- Deploying shared Microsoft security patches
- Checking of patch status of the plant against current threat situation
- Operating a malware protection infrastructure
- Deploying shared anti-virus patches
- Threat monitoring mirrored against the current virus definition standard
- Proactive customer information about incident and short reaction times
- Remote Support
- Complete patch management process monitoring
- Monitoring of the backup infrastructure in the customer’s plant
- Checking for errors and function of the backup process
- Recovery of individual system components / files / system nodes

---

02 Cyber Security Dashboard

---

2 | Cyber Security Services
**ABB Ability™ Collaborative Operations Center**

Within ABB, new Collaborative Operations Center experts will work together to continuously monitor your cyber security and initiate immediate action in the event of an attack.

---

### Further solutions and features of the ABB service

- **Possibility of on-site monitoring by implementing the appropriate infrastructure**

- **ABB is a strong partner for cyber security services**

- **Years of Experience in Control System and cyber security**

- **Strong service structure available for our customers**

---

**03 Process Cyber Security Services**

---

**04 Procedure Cyber Security**

---

**Identify**

Identify security relevant weaknesses in your plant.

---

**Protect**

Protect your assets by implementing basic measures such as system hardening, network security, virus protection and patch management.

---

**Detect**

Detect deviations from the defined security standard and make the right decisions to eliminate cyber threats.

---

**Respond**

Respond immediately to a cyber attack on an affected system.

---

**Recover**

Backup and restore automation systems reliably.