OIL, GAS AND CHEMICALS

Cyber Security Life Cycle Management

Protect your control system against security threats

Cyber security is an integral and continuous part of the product life cycle, from early design and development, through testing and commissioning, to lifetime support. For any life cycle phase, ABB Cyber Security Life Cycle Management helps create a barrier against intrusion.

—
Comprehensive cyber security

Overview

ABB Cyber Security Life Cycle Management is a combination of software and services that mitigate the risk of unauthorized use, access, disruption or modification to the control system.
It helps identify, mitigate and monitor system vulnerabilities to thwart attacks or misuse and ensures that the process control system is operated according to best practices based on international standards and ABB experience.

Benefits

- Enhances risk mitigation against a cyber security attack and system or human error.
- Improves system availability by ensuring production remains uninterrupted.
- Increases plant, environment and community protection.
- Helps ensure compliance with international standards andinternal security policies.
- Provides comprehensive overview of cyber security status.

Services and support

No matter where you are in your cyber security strategy, ABB has comprehensive offerings to fit your needs.

Diagnose: Comprehensive view of cyber security status to understand strengths and vulnerabilities.

- Cyber Security Benchmark:
  - Collects data to identify areas of your control system that are vulnerable to security breaches.
- Cyber Security Fingerprint:
  - Identifies strengths and weaknesses for defending against a cyber attack.
- Cyber Security Assessment:
  - Obtains detailed information about the security of the infrastructure, review of technical documentation, policy and requirements; this is an indepth survey added to the fingerprint.

Implement: Deploy solutions to mitigate vulnerable areas and take proactive measures to prevent in appropriate use or access of the control system.

- Security Patch Management:
  - Specifies requirements and recommendations for implementation and deployment of system security updates for third-party software.
- Malware Protection Management:
  - Specifies requirements and recommendations for implementation and deployment of antivirusupdates.
- User & Access Management:
  - Ensures users always have the approved and relevant access rights.
- Backup & Recovery Management:
  - Provides strategy development for recovery, including robust backup system that can provide system restore to ensure business continuity.
- Network Security Management:
  - Builds a robust network, including firewalls an controlled interfaces to protect against outside intrusion.

Sustain: Security Monitoring and execution of scheduled maintenance.

- Cyber Security Monitoring:
  - Continuous, remote monitoring and periodic security reviews, including alarm triggers.
- System Security Management:
  - Live security monitoring of assets along with performing preventive measures, and actionable intelligence. Keep you control system safe and secure.
- Cyber Security Maintenance:
  - Defines maintenance modules for safe control systems.

Consulting: Specialist counseling

- Security Risk Assessment:
  - Follows IEC 62443 based process for performing a cyber security risk assessment.

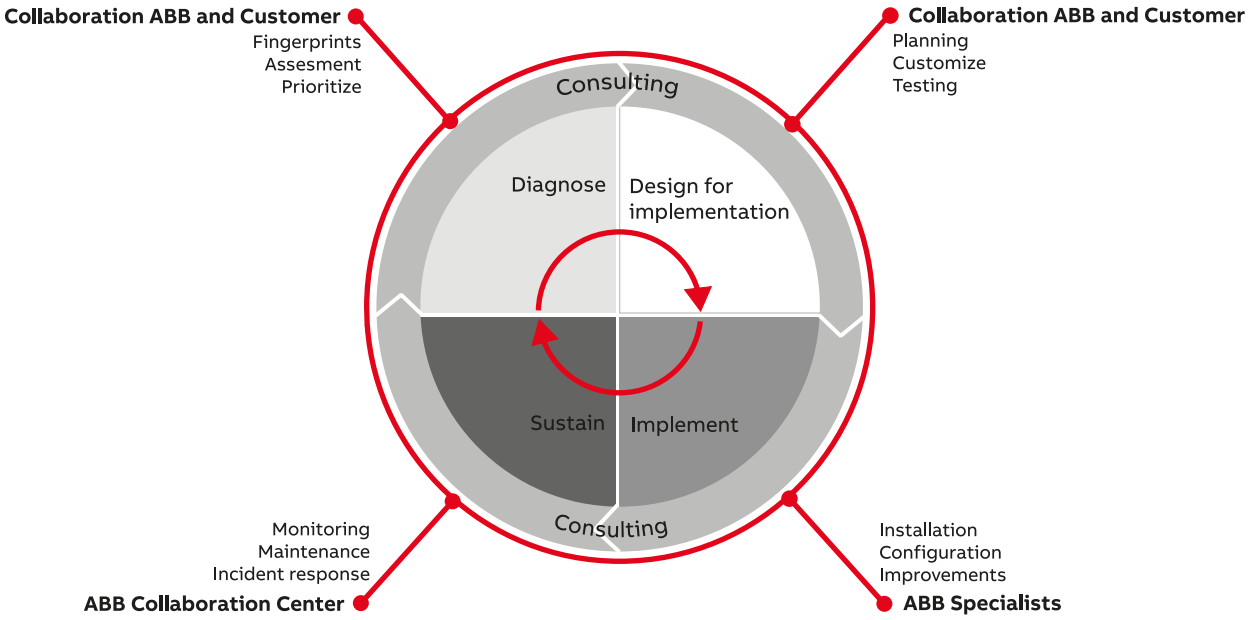

ABB AS
Ole Deviks vei 10
Postboks 6359, Etterstad
N-0603 Oslo, Norway
Contact center: 03500 / +47 22 87 20 00
Email: contact.center@no.abb.com

abb.com/oilandgas

9AKK 106713A6256 - 01