BROCHURE

Cyber Security Risk Assessment

Cyber Security Risk Assessment Service

—
01 The risk of cyber attacks on industrial targets is expected to increase as the Fourth Industrial Revolution takes hold

Overview
Cyber attacks against industrial control systems are rising. Hackers, organized crime, nation states, insider threats, malware and viruses all pose serious threats to industrial producers that depend on automation.

ABB's Cyber Security Risk Assessment is designed to counter these threats. The assessment helps plant operators and facilities managers uncover, rate, prioritize and remedy control system cyber security risks by providing them with a detailed in-depth view of their control system's security posture and risk mitigation strategy.

Conducted in accordance with the best practices outlined in the ISA/IEC 62443 standards for securing control systems, assessment teams conduct a high-level cyber security risk assessment of the system-under-consideration to determine and assess system-wide risks.

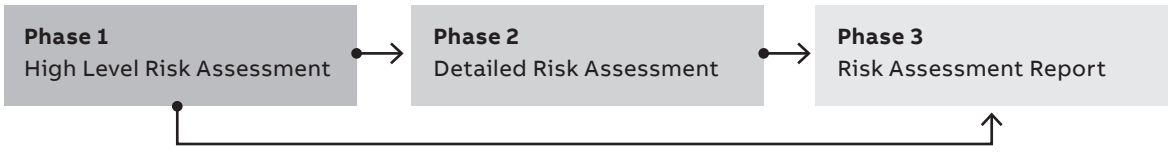
The results are used to partition the control system into zones and conduits. A detailed risk assessment is then conducted for each zone and conduit. The result is a cyber security action plan operators can use to prevent the disruption of operations by even the most determined attackers.

Benefits
- Clear understanding of control system vulnerabilities
- Improved control system risk management
- Improved risk mitigation and containment

—
01

CSRA Service In-Practice
The service is carried out in three phases:

- **Phase 1** – High Level Risk Assessment
- **Phase 2** – Detailed Risk Assessment
- **Phase 3** – Risk Assessment Report



Phase 1 – High Level Risk Assessment
Examines the potential impact cyber security vulnerabilities have on the control system as well as the likelihood of those vulnerabilities being exploited by an attacker. The aim is to expose worst-case scenarios should those systems or sub-systems be compromised.

The process involves conducting an in-depth risk analysis workshop to gather input from stakeholders and identify risks. Input from stakeholders will include an overview of the system architectures and functions along with knowledge-sharing regarding specific types of incidents that have occurred in the organization.

This work will generate a prioritized list of cyber security risks, based on an analysis of the vulnerabilities and threats to the different assets in the control system.

Using this information, control system boundaries are established and system assets and subsystems are identified.

The output documentation includes a zone and conduit diagram as well as a list of scenarios that describe how threats could take advantage of existing control system vulnerabilities.

In some cases, it can be enough to perform just this portion of the assessment. If this is the case, a report is generated including a diagram of risk for zones and conduits. Depending on the risks identified, a more detailed investigation may be needed. If so, a Detailed Risk Assessment will be conducted.

Phase 2 – Detailed Risk Assessment
Based on the zone and conduit diagram produced by the High-Level Risk Assessment, detailed cyber security assessments are conducted for each zone and conduit that takes into account existing controls. Threat and risk scenarios are then developed and analyzed for each asset.

Phase 3 – Risk Assessment Report
Phase 3 consists of documenting the site's cyber security requirements, assumptions and constraints. This information is combined with the risk treatment plan and descriptions of recommended actions to create the Risk Assessment Report. System upgrades required to reduce risk of attack to an acceptable level will also be proposed.

—
02 Example documentation of cyber security requirements, assumption and constraints resulting from a Cyber Security Risk Assessment

—
02

Documentation

Requirements	What are the zones, conduits and target security levels
Assumptions	What assumptions was the risk assessment based on
Constraints	What legal or functional restrictions do the selected systems have
Design	What is the design of the system
Manuals	How to conf igure, monitor, maintain and administer the control systems
Training	What training is required to keep the system secure
Change Management	Risk-assess and document all changes to the system and operating procedures

Design

Devices	What devices make up the system and where they are located
Users	Who is allowed to use the system and what is their security access level
Network	What devices are connected to which ports at what addresses
Configuration	What security setting are configured into the system

ABB IAOG
Ole Deviks Vei 10
N-0601 Oslo, NORWAY
E-mail: contact.center@no.abb.com

abb.com/oilandgas

9AKK107245