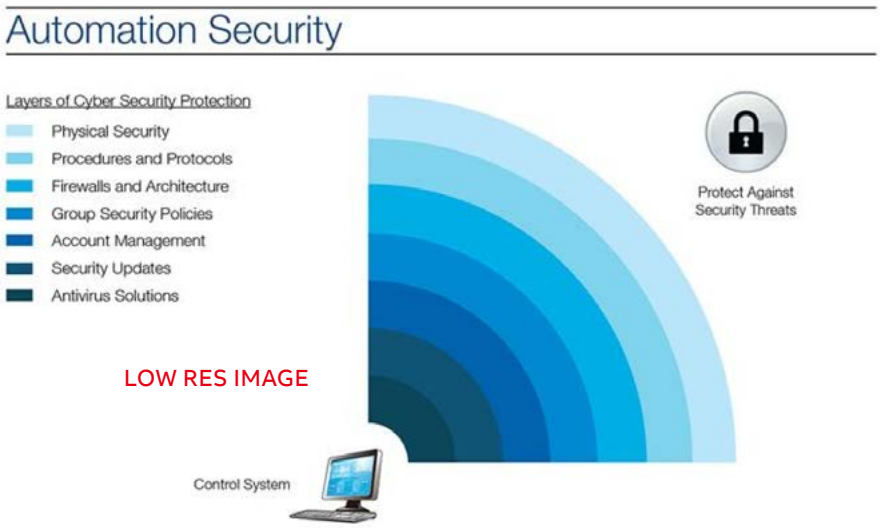
FSM TECHNICAL AUTHORITY

Safety Instrumented Systems

Cyber Security Risk Assessment for SIS



LOW RES IMAGE

The safety standards IEC 61508 and IEC 61511, have requirements to address cyber security in safety instrumented systems (SIS). This is because in today's world, neither functional safety nor information technology are independent of one another.

The question to ask is, 'how do we make the SIS cyber secure?' This is not a single task assignment but it requires properly aimed and controlled activities to be provided at all stages of the functional safety life cycle. Safety and cyber security have similar and co-dependent thought processes. There are specific roles and responsibilities required from manufacturers, certifying bodies and system operators. This forms a life cycle process for cyber security akin to the functional safety life cycle as identified in IEC 61511

It therefore follows that industry should be immediately implementing an 'integrated' safety and cyber security life cycle management approach to ensure safety systems are adequately secured across the conceptual, design, engineering, installation, operation and maintenance of control and safety systems.

IEC 61508 from 2010, and the recently issued IEC 61511 edition 2, have requirements to address cyber security vulnerabilities of the SIS during the process hazards and risk assessment and to implement into SIS cyber security countermeasures during SIS design. Refer to IEC 61511 Part1, clause 8.2.4 and 11.2.12

The lack of and/or or inappropriate security risk assessment can affect the security countermeasures of the SIS and may result in security hazardous events that have significant consequences on plant operation disruption or damage, personnel injury or fatality.

Background to the ABB Approach

ABB's cyber security services enables asset owners to become conversant with the relevance of cyber security requirements for the SIS in the context of a broader security policy for the entire automation and business management systems deployed at site.

The Approach

Effective risk assessment requires input and operational experience contribution from many disciplines. Utilising a competent study leader and an appropriate number of relevant disciplines such as the responsible Instrumentation Engineer, Information Technology Engineer, Operational and Project Management/Supervisory representation, we can provide effective guidance to obtain maximum benefit for the study outcome.

The risk assessment will detail each potential vulnerability and assess the identified threats in terms of potential likelihood and consequences. Where the achieved risk is not tolerable, then the determination of additional risk reduction countermeasures shall be identified and applied.

The findings of the risk assessment can then be further utilised to establish the necessary requirements with the Safety Requirements Specification (SRS) and Functional Design Specification for the proposed SIS.

Benefits of ABB Cyber Security Risk Assessment for SIS

- Supports the extensive application and compliance requirements for demonstrable knowledge of safety instrumented systems, the legislation concerned, the regulatory perspective and also the standards/criteria against which a company/system will be measured.
- Demonstration, that effective and robust risk assessment is being taken, shows the pro-active attitude which is expected by the authorities, public and workforce, and supports company risk management arguments.
- Provides traceability of the risk assessment and operational management process for both Greenfield and Brownfield operations, thereby demonstrating the necessary risk mitigation to be implemented in the cyber security execution process.

ABB Cyber security services

Functional safety and cyber security are given the highest priority in all of our products, systems and services. Cyber security is an integral and continuous part of the product life cycle, from early design and development, through testing and commissioning, to life time support service and future adaptations. Cyber Security Services ensure that the control and protection systems are operated according to best industry practices based on international standards and ABB experience. Our overall offerings include:

- System Benchmarking to identify areas of your industrial automation system that are vulnerable to security breaches
- System Fingerprints to identify strengths and weaknesses for defending against cyber attacks
- Cyber Security Assessment Survey to obtain information on existing cyber security measures
- Control System Compliance Review for security status evaluation
- Implementation of protection, backup & recovery management
- Provision of monitoring, periodic reviews and maintenance measures to keep industrial automation systems safe and secure

Assured and certified products, services, delivery and execution

For further information, please contact:

ABB FSM Technical Authority
Howard Road, Eaton Socon, St Neots
Cambridgeshire, PE19 8EU
Phone: +44 (0)1480 475321
E-Mail: oilandgas@gb.abb.com

www.abb.com/oilandgas
www.functionalsafetyinsights.com

SIS Cyber Security Risk Assessment / 3BGB 000945 D0001 / November 2017