—

ABB Cybersecurity.
A brand of trust.

The advent of the digital age and advanced control systems enable utilities and industries to measurably enhance profitability without compromising operational safety, availability, or resilience.

The myriad of advantages associated with digital growth expose a long-standing problem with operational technology; exposure to increased cyber risk. In addition, the threat of cyber-attack has become ubiquitous and is now a common C-suite and board level topic, regardless of business vertical. Cyber risk is manageable and is a critical component of any digital transformation. This document highlights the core beliefs that underpin ABB's approach to cybersecurity and keeping our customer's operational integrity and data safe. At the center of our methodology are people, process, and technology.

The Trusted Partner

Cybersecurity concerns can become particularly acute when businesses attempt to integrate new and legacy systems without taking a holistic approach to cybersecurity.

ABB has long been a trusted partner for industrial automation and control technology. We bring our rich heritage and deep understanding of the industries we serve and the challenges they face. There are more than 70 million connected devices, 70,000 digital control systems and 6,000 enterprise software solutions delivered by ABB around the world. As a leader in the industrial space, we have four decades of experience creating secure digital solutions for customers in across all sectors of industry. The slightest interruption in any industrial system can have massive consequences for the environment and economic activity.

Over the years, cybersecurity has become an integral part of ABB's product portfolio. Today, it is front and center at every phase, from design and development to product maintenance and support.

Holistic Approach

When it comes to cybersecurity, we are living in the age where companies have been besieged from every angle with the cyber threats. But as the digital age matures it is now time to start talking about security as a fundamental design consideration that is built into our products from the outset. The industry is also facing the challenge of how to address the retrofit or upgrade for the vast legacy environments that were designed and installed before cybersecurity was a priority. ABB provides guidance, products, and services to address both scenarios – for both green field and brown field applications.

At ABB, cybersecurity is a built-in capability that comes as a given in all our products and services, much like seatbelts and airbags in a vehicle.

Secure Reference Architecture

As part of our cybersecurity offering in industrial automation, we have developed what we call our Secure Reference Architecture and standard. This is a template for the entire ABB control suite and builds on the implicit level of trust that industry has on ABB to deliver effective technologies and solutions. It covers everything from access control definitions to data flows. We have built on our many years of expertise in deploying and maintaining these systems and have built a new layer around that which defines how to deploy the technology, configure it and manage it securely.

The ability to visualize both an architecture level and on a deeper technical level allows us to add extra layers of security and functionality such as remote access to the design.
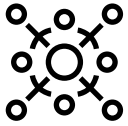
Industrial Partnerships and Collaboration

The control landscape contains many third-party tools and solutions that can be integrated and validated within our Secure Reference Architecture design. The validated design can be achieved thanks to trust in our domain knowledge and technical expertise that has been established over decades of experience. We see it as our responsibility to help our customers who select third party suppliers in integration and validation as part of our design strategy. Our expertise allows us the ability to source and select best of breed and gives us the flexibility to apply equivalent or better technology when market or technology conditions dictate.

As a company we are aware that you cannot operate in isolation. ABB has its deep domain and technology pedigree, but to deliver an integrated technology package we work closely with key technology partners. These partnerships are critical to our vision, both from a business and a technology perspective. Now and in the future, we will partner and collaborate with key technology providers that will allow us to deliver together this integrated technology and commercial vision.

More than Standards

Effective cybersecurity is more than simply adhering to standards and regulations. While ABB understands the important role that regulations such as IEC 62443, NIST 800-82 and ISO 27002 play in ensuring cybersecurity compliance, we approach this from another angle. We are fully alert of these standards and familiar with their requirements. Our role is to ensure that our design and configuration will fully support customers with the compliance that they require, following their chosen standard.

Response

ABB realizes that its customers are concerned about protecting and minimizing the risk of a cybersecurity incident. While asset owners have the prime responsibility for any incident response procedures, ABB actively monitors for any cybersecurity threats that may have an impact on ABB control systems, as well as proactively communicating to customers when deemed critical. ABB also facilitates a mechanism for customers to communicate any potential concerns or threats to the product security group to allow two-way communication.

Summary

Cybersecurity comes down to people, process and technology. ABB has the domain knowledge and experience to provide the defense-in-depth security that is a prerequisite for modern companies. As the digital age becomes more mature it is apparent that cybersecurity means much more than protection against cybercrime: certainly, connections need to be safe, but the value of that data should also be protected. Customers should not be required to forfeit safety, value, or control in order to realize the benefits of digitization, and ABB closes the loop between these needs with an innovative, multi-layered approach to security.

8VZZ000367T0047