At the center of ABB's methodology are people, processes, and technology. ABB has long been a trusted partner for industrial automation and control technology and has a deep understanding of the industries it serves and the challenges they face. Around the world, the company has delivered more than 70 million connected devices, 70,000 digital control systems and 6,000 enterprise software solutions. As a leader in the industrial space, it has four decades of experience creating secure digital solutions for customers across all sectors of industry.

Over the years, cybersecurity has become an integral part of ABB's product portfolio in much the same way as seatbelts and airbags have become an indispensable element in every vehicle. Today, cybersecurity is front and center at every phase, from design and development to product maintenance and support. Furthermore, this applies not only to new installations but to legacy facilities as well. Indeed, many industries are facing the challenge of how to retrofit or upgrade legacy environments that were

As the advantages associated with digital services have proliferated, so too have the risks of cyber-attack. Indeed, the threat of such attacks has become ubiquitous and is now a common C-suite and board level topic, regardless of business vertical. Nevertheless, cyber risks are manageable, and their control is a critical part of any digital transformation. This article highlights the core beliefs that underpin ABB's approach to cybersecurity and to keeping its customers' operational integrity and data safe.

Ragnar Schierholz
Cybersecurity Council, Industrial Automation
Minden, Germany
ragnar.schierholz@de.abb.com

Robert Putman
Cybersecurity Council
Products and Service
Zurich, Switzerland
robert.putman@ch.abb.com
designed and installed before cybersecurity was a priority against targeted attacks and so-called white noise attacks (see box →01). With this in mind, ABB provides guidance, products, and services to address both green field and brown field applications →02.

Secure reference architecture
As part of ABB’s cybersecurity offering in industrial automation, the company has developed a Secure Reference Architecture and standard. This is a template for the entire ABB control suite and builds on the company’s ability to deliver effective technologies and solutions.

—

ABB has four decades of experience creating secure digital solutions for customers across all sectors of industry.

Covering everything from access control definitions to data flows, ABB’s Secure Reference Architecture is based on years of expertise in deploying and maintaining such systems. It defines how to configure and manage technologies securely, and, thanks to its ability to visualize architecture levels, allows users to add layers of security and functionality, such as remote access, to a design.

Industrial partnerships and collaboration
The control landscape contains many third-party tools and solutions that can be integrated and validated within ABB’s Secure Reference Architecture design. Validated designs can be achieved based on the company’s domain knowledge and technical expertise. In addition, as part of its design strategy, the company helps its customers select third party suppliers to optimize their integration and validation and to source and select best-of-breed solutions while applying equivalent-or-better technology as market or technology conditions evolve. Furthermore, in order to deliver an integrated technology package, ABB works closely with key technology partners. These partnerships are critical to the company’s vision from a business as well as a technology perspective.

More than standards
Effective cybersecurity is more than simply adhering to standards and regulations. While ABB understands the essential role that regulations such as IEC 62443, NIST 800-82 and ISO 27002 play in ensuring cybersecurity compliance, it works closely with its customers to ensure that
its designs and configurations will fully support its customers’ compliance needs based on their chosen standard.

ABB realizes that its customers are concerned about protecting against and minimizing the risk of a cybersecurity incident. While asset owners have prime responsibility for any incident response procedures, ABB actively monitors for any cybersecurity threats that pose a potential impact to ABB control systems. It also proactively communicates with customers when a situation is deemed to be critical and maintains a mechanism whereby customers can communicate any potential concerns or threats to the ABB product security group via two-way communication.

All in all, ABB is well positioned as a systems integrator – a factor that is foundational to the company’s cybersecurity strategy in the industrial controls arena. There are two aspects to this. The first is that the customer can trust that implementation of a 3rd party solution in ABB’s reference architecture will result in optimal value.

The second is that the customer can rest assured that if there is a failure or a problem with implementation, it will, in all probability, not impede the availability or safety of assets and will ease their recovery.

**Achieving the full benefits of digitization**

Cybersecurity comes down to people, processes, 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 the associated data should also be protected. ABB’s view is that customers should not have to forfeit safety, value, or control in order to realize the benefits of digitization. With this in mind, ABB closes the loop between these needs with an innovative, multi-layered approach to security.