01

DATA CENTERS

Security beyond the borders – data center cyber security

Cyber security is woven throughout the ABB Ability™ Data Center Automation solution and includes product design, project execution and operation. ABB supports data center customers to secure networks, servers and data in addition to perimeters.

To operate dependably and efficiently, data centers require their electric infrastructure as well as the building automation and industrial control systems (ICS) that manage this infrastructure to deliver an uninterrupted power supply (UPS). Integration of Operational Technology (OT) with Information Technology (IT) leads to greater reliability, control and enhanced performance, but also exposes data centers to unprecedented challenges: cyber threats. The real possibility of malicious entities or persons accessing mission-critical systems like data centers that rely on connected controls creates raw angst and this can drive the market. For instance, the global industrial cyber security market, which includes network security, industrial control systems (ICS), hardware- and software solutions, is expected to hit USD 24.41 billion for the period between 2017 and 2023 [1].

A decade ago, data centers focused solely on securing their physical perimeter and the data they stored and managed.

Today, the data center cyber security landscape is diverse, whereas a decade ago centers focused exclusively on securing their physical perimeter and the data they stored and managed (information security). Open IT standards for automation systems that encourage connectivity to external networks were not yet established and enterprise data centers dominated the landscape. What was sensible then is now alarmingly insufficient. Nowadays, data centers include cloud-based servers and interconnected ICSs that expose cyber risks not previously encountered. Currently, perimeter and data security are not enough to protect data centers from failures and blackouts [2].

ABB applies a comprehensive approach to cyber security for data centers with security woven throughout the design, development and deployment phases of industrial automation and control systems, including all electrification products. Relying on international standards and a knowledge-based systematic approach, ABB uses best practices to ensure that cyber security has a starring role in its data center automation products.

As the largest enterprise asset management and distributed control system (DCS) supplier in the world, with a 20 percent market share [3], ABB is ideally suited to provide reliable and secure automation and control systems while maintaining transparency and interoperability. ABB achieves these goals with its Data Center Automation solution, thereby supporting the availability and continuous optimization of data center mission-critical systems and products. ABB's automation system provides core technology for the ABB Ability™ Data Center Automation solution for on-premise and hybrid cloud environments.

Thus, ABB can deliver industrial strength, mission-critical converged solutions for mechanical controls (BMS), electrical monitoring (EPMS), electrical controls (ECS) and Data Center Infrastructure Management (DCIM) to data centers. This open platform allows automation and data exchange among systems, equipment, components and applications to:

- Integrate data center tool sets faster; this includes the ability to upload assets into tracking tools.
- Visualize and manage physical assets within a 'single pane' view of the entire data center, including multiple sites.
- Automate cooling and electrification systems for continuous optimization and improved uptime.

Cyber threats: the nitty-gritty reality

Over the past decade, the severity and sophistication of cyber threats toward existing ICSs and associated infrastructure have increased [4]. While industrial communication involves a myriad of hardware and software products and protocols to establish communication between industrial automation devices and standard computer platforms, systems were originally built to meet performance, reliability, safety and flexibility requirements without much thought to secure communication capabilities. By focusing solely on securing perimeters and data, these legacy ICSs and their infrastructure are woefully pervious to cyber attacks and incidents.

Despite this predicament, companies must exploit real-time process- and system information to increase the interconnectivity and predictable interoperability between different automation systems, and combine legacy systems with new ones. This communication landscape raises the level of security threats that data center customers face dramatically.

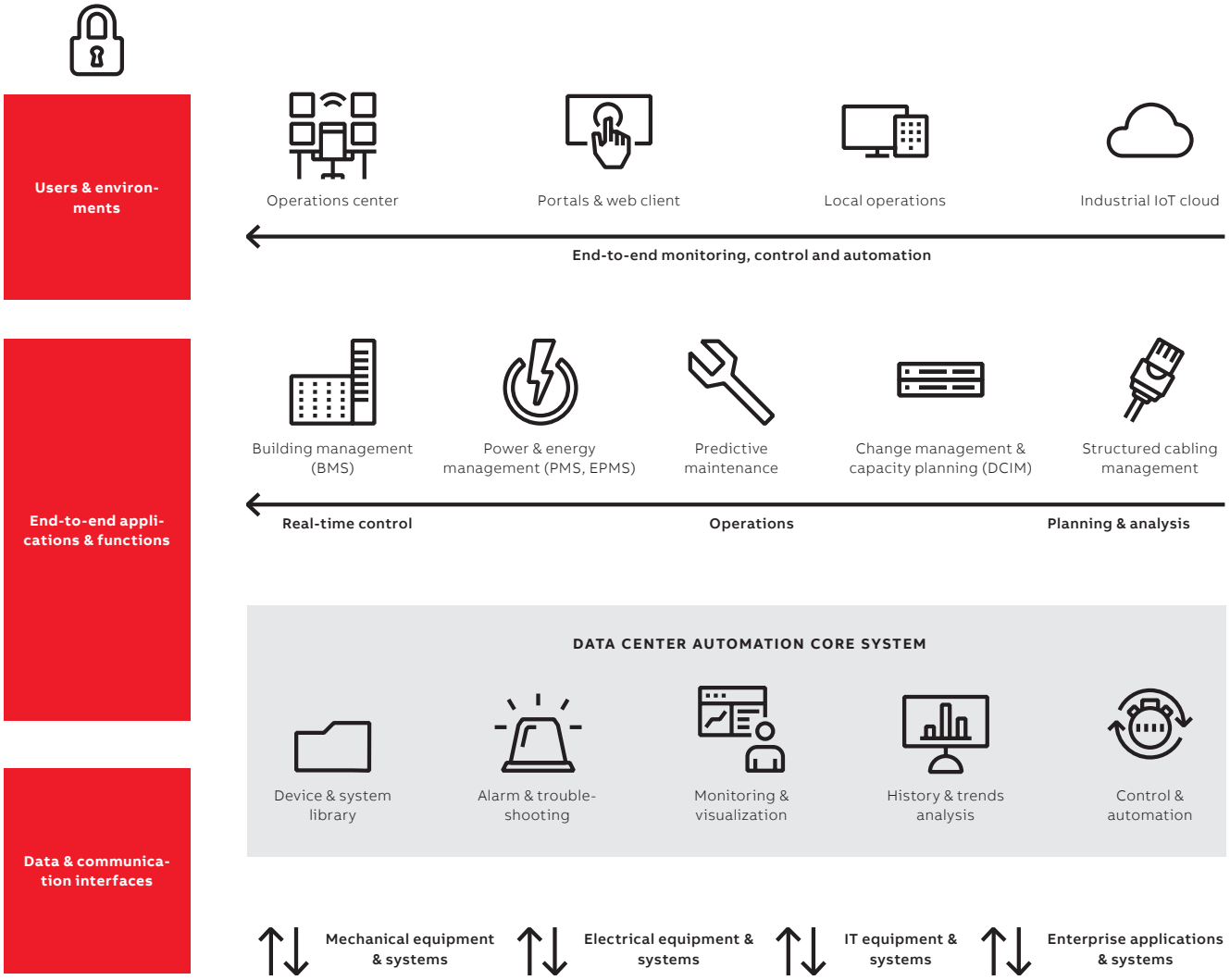
Nowadays, electrification infrastructure and industrial controls are an integral and continuous part of the entire ICS system lifecycle from

Madhav Kalia
ABB Data Center Automation Solutions
Singapore

madhav.kalia@sg.abb.com

Apala Ray
ABB Industrial Automation Process Industries
Bangalore, India

apala.ray@in.abb.com



01

design and development, through testing and commissioning, to lifetime support service and future adaptations. By providing holistic cyber security solutions, ABB helps customers on their journey to identify, mitigate and manage changing cyber risks that could impact their systems. ABB's cyber security approach for all offerings, including data centers, focuses on three areas: product design, project execution and plant operation.

Securing data centers: recognizing the challenges

The upswing in intense and diverse cyber threats experienced recently, require networks, servers, data and perimeters to be secure [2].

Perimeter security includes safe-guarding the electric infrastructure and controls by means of mechanical and/or electronic systems in addition to safe-guarding the physical perimeter. Because security management within a facility is coupled with individuals and their roles, having employees with different authorization roles is a crucial challenge.

In addition, industrial and proprietary protocols often lack proper measures for data security of electric infrastructure and controls, eg, authentication or integrity checks; or support of cryptography mechanisms.

It is also quite a feat to secure the communication network and protect data from attacks originating from any other communication

—

The recent upswing in intense and diverse cyber threats require networks, servers, data and perimeters to be secure.

network; this includes cryptographic operations management. Additionally, to ensure client and server security for electrical infrastructure and controls, patches must be applied and

snit-malware definition files used to scan. And, if an unforeseen disaster strikes, proper backup mechanisms must allow recovery. Virtual environments are especially challenging and require excellent monitoring solutions. ABB provides safeguarding solutions to address all these challenges.

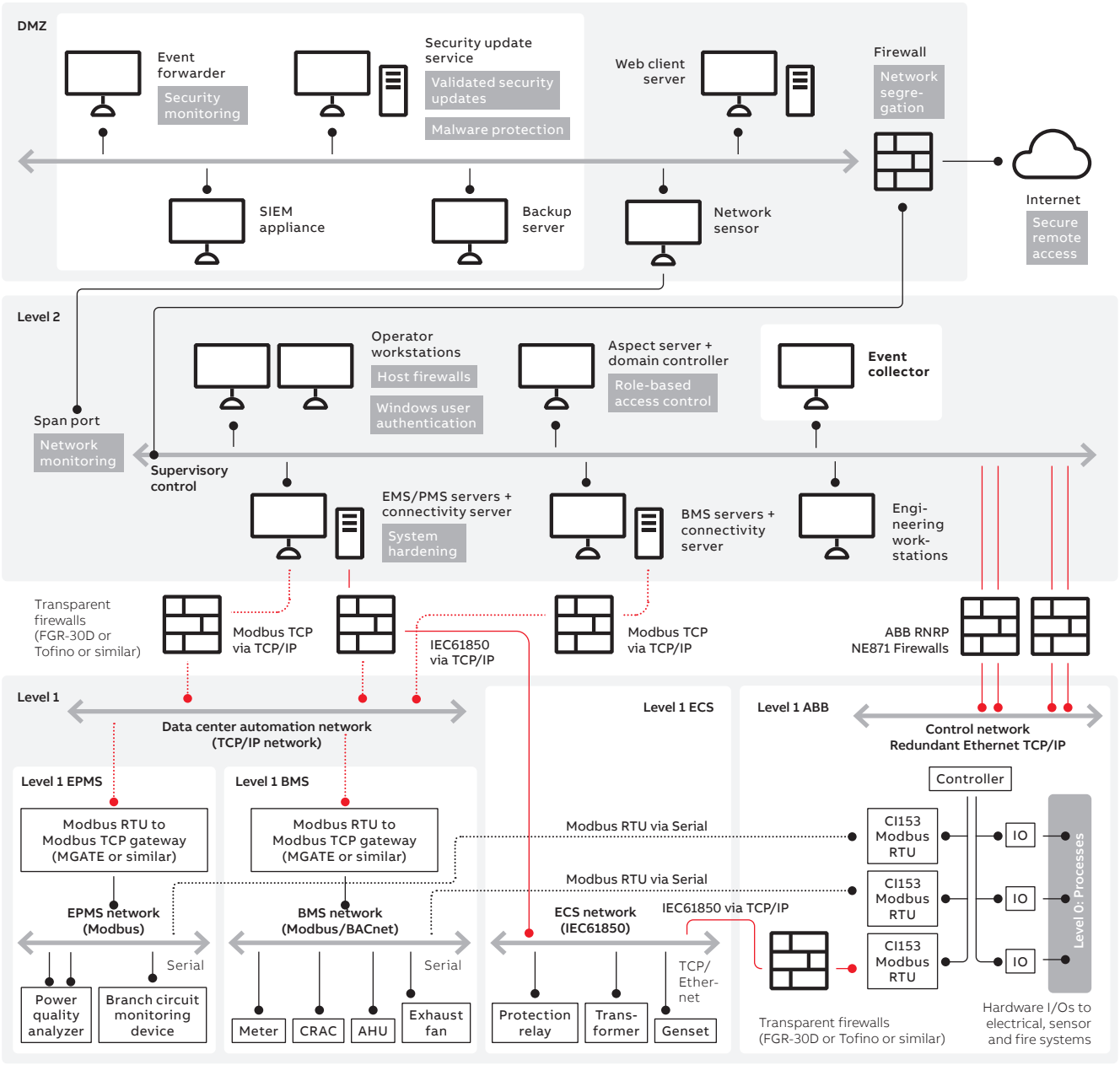
ABB's cyber security solution for data centers

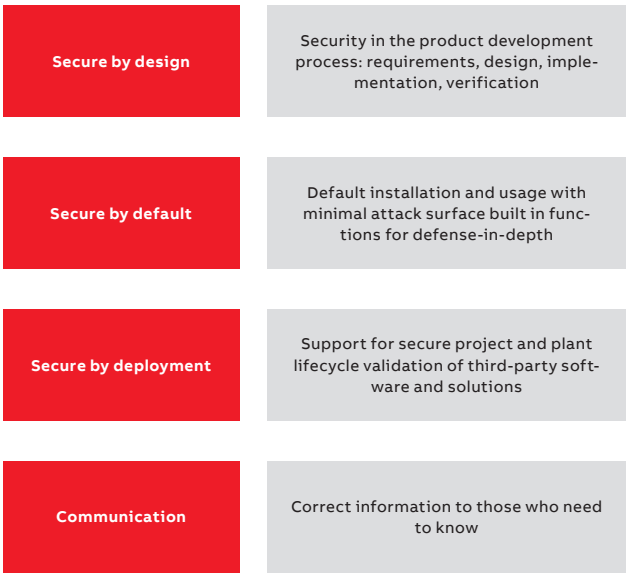
ABB's Ability™ Data Center Automation solution provides customers with the means to engineer, commission, monitor, control and operate automation strategies for their systems, →01 by delivering ECMS that include Energy Management System (EMS), Building Management System (BMS) and Power Management System (PMS). ECMS capture all information/data for the purpose of recording, controlling and reporting.

Clearly, technology alone cannot eliminate cyber risks. By defining the means to deploy a data center automation system with the appropriate security controls, ABB supports customer's cyber security efforts →02. ABB's reference architecture can also be customized according to individual project requirements. To accomplish this, customers should contact ABB's project team. Thus, people, processes and technology are at the heart of ABB's fortified cyber security approach.

—
01 ABB Ability™ Data Center Automation system architecture provides customers with automation strategies for all their power, electric, mechanical and building systems.

—
02 Schematic of a reference architecture for ABB's cyber-secured Data Center Automation solution.





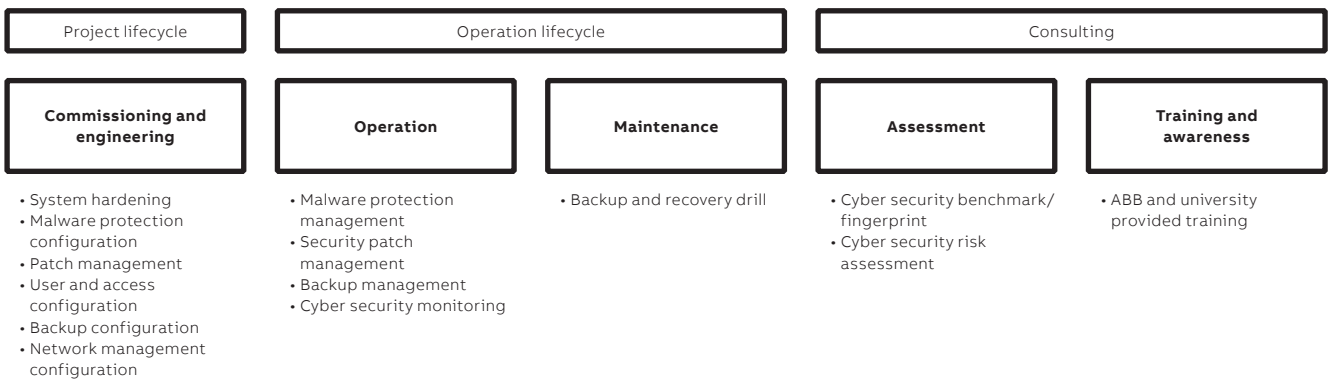
03

Secure by segregation

ABB's reference architecture places all the components of the data center in a specific network level →02. This widely used security concept segregates secure from insecure networks with firewalls and demilitarized zones (DMZs). For data center automation systems, the internal network has different devices with varying security levels; here, network zoning with a hardened system is critical. Network connectivity within a level is governed by the host firewalls (software firewall residing on individual computers); data can only pass to another level via a (hardware) firewall. The ABB data center architecture implements user-, software- and device authentication; account management, authorization enforcement, malicious code protection and network segmentation and continuous network monitoring to ensure against cyber incidents →02. The operation and maintenance phase of the data center automation lifecycle with different security controls are part of ABB's architecture →02. This layered approach uses different cyber controls to successfully address security issues at the server-, network- and data level:

ABB's cyber security approach focuses on three areas: product design, project execution and plant operation.

- Patch management – by using validated system security updates of the server from third-party software, namely, Microsoft, EXSi and Adobe products, users can be confident that the control system is always updated.
- Anti-virus updates – servers should include the latest updates.
- Backup management – includes documentation of procedures, testing of backups, and storage of qualified backups in a safe offline location; thereby ensuring that system failures or extended downtime do not result in loss of data. ABB supports applications that schedule, manage and operate data backup processes on computers, servers or network devices regularly. These steps are in accordance with the organization's system recovery plan.
- Hardening – the hardening process reduces the attack surface, the number of software applications, disables non-essential services, utilizes host firewalls, and changes default passwords. Only necessary applications and services are installed.
- Manage user accounts and user access rights and roles – a critical security challenge.
- Monitor the automation systems with the security information and an event management



04

platform – new threats emerge continually and intrusions happen daily, so continuous monitoring keeps control systems safe and secure.
- ABB adheres to the SD3+C Security Framework, created by Microsoft to ensure and improve security of its products; →03, eg, reduce the number of security bugs or vulnerabilities present in new software; make default product installations and configurations more resistant to attack; ensure that products can be installed, configured, operated and maintained securely; and promote responsible communication.

Delivering the best possible value

Cyber security services are integrated within the lifecycle of ABB Ability™ Data Center Automation solution and include: project execution lifecycle, operation lifecycle and consulting services →04. The commissioning and engineering phase can provide a onetime configuration for the cyber security setup, whereas the plant life cycle deals with the renewal of cyber security services for regular operation and maintenance.

These cyber security services ensure that the data center infrastructure is operated according to best practices that are based on international standards and rely on ABB's vast experience. The goals are to verify, provide, address, and support:
- Verify that updates do not interfere with the operation of the data center infrastructure system.
- Provide services with consistent quality and assure that tasks are performed by skilled personnel.
- Address cyber security throughout the development lifecycle of ABB products and solutions.
- Support security throughout the operation lifecycle of the solutions delivered by ABB.

Customer concerns and the way forward

Ensuring network-, server-, data- and perimeter security for electric infrastructure and controls is what data center customers need now and in the future. Because the network segregation is a primary objective of ABB's reference architecture →02, firewalls are used to control and moderate the traffic in different network levels; this improves the network traffic visibility. Network security is also improved through network monitoring to allow the detection of unusual events.

A three-stage model has been established for cyber security management of ICS environments. The first stage is to establish a basic level of technical and organizational security controls. If those controls are suitably implemented and maintained, they will thwart the majority of generic threats. The second stage is to continuously manage and maintain these controls and add more sophisticated controls as needed. The third stage is the collaborative operation of cyber security controls with managed security services via ABB's Collaborative Operations Center.

ABB's reference architecture implements user-, software- and device authentication, account management, authorization enforcement, and malicious code protection to improve the posture of security levels in the server. Regular updates of security-patches and anti-malware definition files also improve the security postures. The backup management server in DMZ enables data backup and recovery from catastrophic incidents using ABB's recommended platform. Ensuring data security for the electric infrastructure and controls is a top priority as is perimeter security. The secure, encrypted and compressed data transfer between data collector node and history server enables secure communication; event monitoring occurs in ICS. To ensure perimeter security for the infrastructure and controls, ABB recommends enforcing physical security while deploying the automation system in data centers.

ABB delivers data center customers innovative solutions that resolve the most vexatious cyber security challenges.

ABB's cyber security efforts don't end with this comprehensive approach. ABB recognizes that cyber threats will continue as cloud adoption expands. Currently, ABB's experts are exploring a tamper-proof solution: a trusted platform module, that stores Rivest-Shamir-Adelman (RSA) encryption keys. Such a solution will provide customers with a safe computing environment for the cloud. Hence, ABB delivers data center customers innovative solutions that resolve the most vexatious cyber security challenges today and tomorrow. •

03 SD3+C Security Framework is depicted.

04 ABB's data center cyber security value chain is illustrated.

References

[1] Market Research Future, "Industrial Cyber Security Market Worth 24.41 USD Billion By 2023 With 10.97 % CAGR", Market Research Future, Sept. 28, 2017, Available: https://www.marketresearchfuture.com/press-release/industrial-cyber-security-market [Accessed: June 26, 2020].

[2] F. Howarth, "Architecting the security of the next-generation data center: a white paper by Bloor Research", in Bloor Research, Aug. 9, 2011, Available: https://www.bloorresearch.com/research/ [Accessed: May 5, 2020].

[3] ABB Press, "Industry analyst ranks ABB #1 for distributed control systems globally", Nov. 6, 2018, Available: https://new.abb.com/news/ [Accessed: May 5, 2020].

[4] W. Ashford, "Cyber threat to industrial control systems highest yet", in Computer Weekly, March 2, 2018, Available: https://www.computerweekly.com/news/252436129/ [Accessed: May, 5, 2020].