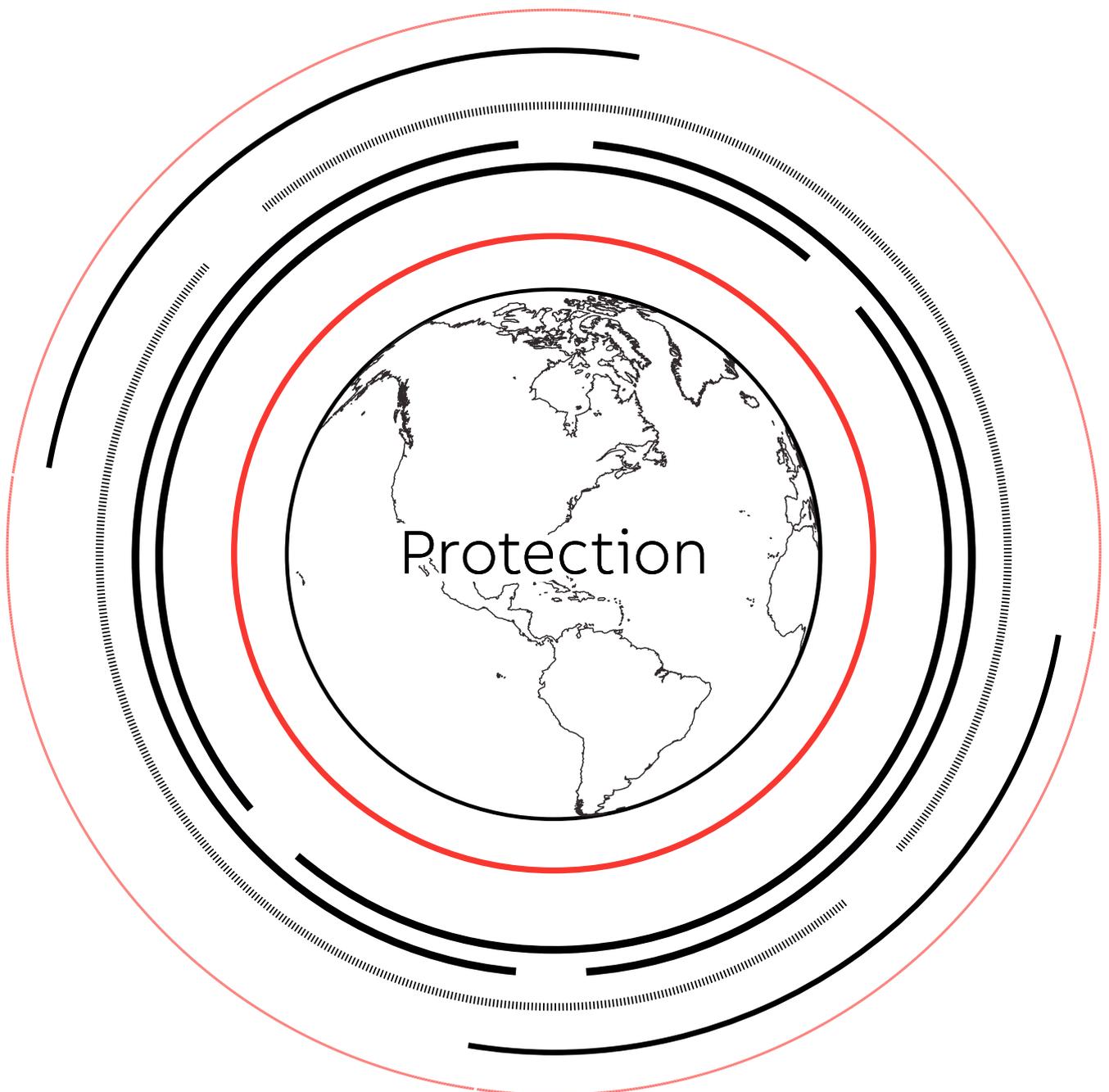


GRID AUTOMATION SERVICE

Enabling smarter system protection.

Cyber Security Care



Three steps to cyber security vigilance.

Helping to defend your grid automation systems.

Every grid automation system is potentially out of date and constantly needs maintaining and updating. By not updating your system you leave yourselves exposed to attack, the threat exponentially increases the longer the system is not maintained and updated.

ABB Grid Automation service offers a three step approach to cyber security to help defend your systems:



Assess

To begin the process ABB carries out a cyber security assessment to help you understand how to improve security throughout your system. A detailed cyber security assessment report is then produced and provided to you along with a set of recommended actions for improved cyber security.



Implement

ABB provides recommended actions for you to implement based on the cyber security assessment and our experts domain expertise. Upon agreement ABB implements the recommendations to your system, ensuring your system is more secure.



Sustain

By appointing ABB as your cyber security partner; you enter a care agreement which ensures you benefits not only from ABB's huge domain expertise across the globe but also your system will be regularly assessed by the cyber security care team for any potential cyber security infringements. This ensures a long term approach is taken to ensure sustained cyber security vigilance.



Security assessment & monitoring

Unique security assessment solutions.

Assessment and monitoring services for system software, system hardware and communication networks are fundamental in order to keep a system constantly secure. Overseeing the cyber security status of your system, ABB's collects system data for comparison against industry best practices and standards to detect weaknesses within your system's defense. This pinpoints areas that require action to help protect your system by ensuring it has multiple layers of security.



Malware Protection

Evolving protection against sophisticated threats

Our substation automation systems can be equipped with industry-standard malware and intrusion protection solutions, like anti-virus protection and application whitelisting.



Procedures & policies

Educating and supporting system users

Cyber Security will always be a challenge on a global scale; no single solution can keep increasingly interconnected systems secure, so ABB works with customers to understand your processes and procedures, group security policies and computer settings to create a defense-in-depth approach where multiple security layers detect and deter threats – if, where and when they may arise.



Backup & recovery

Preserving the past for a rapid response to tomorrow's challenges

If the worst does happen, and cyber-attack or natural disaster strikes, then the security of an off-site back-up will make recovery that much easier. ABB's back-up solutions can ensure the integrity, and availability, of critical data, no matter what happens to the original.



Security updates & hardening

Effortlessly updating and improving your system

Modern operating systems and embedded software often need to be patched to defend against emerging threats. Efficient patch management is an essential part of any security policy, but one that is often neglected. Products can be made significantly more robust by closing ports and services that are not in use. Our products have been systematically hardened to ensure that the products are robust against attacks and perform their main function.



Perimeter protection

Constantly vigilant for attacks and breaches

Firewalls can protect the perimeter of a network and a well-designed security policy will separate the network into distinct, controlled zones, protected by internal firewalls to ensure that a compromised server doesn't mean compromising the entire network.



—
abb.com/cybersecurity