RELION® 670/650 SERIES

Cyber Security

Securing your protection and control devices

- User account management
- Secure communication
- Protocol hardening and patch management
- Supervision and configuration

Cyber Security
Securing your protection and control devices

Continuous development

Anticipating, adapting and applying

Focus on cyber security has steadily increased in the electric sector over the last couple of years.

ABB is committed to providing customers with products and systems that clearly address cyber security and thus constantly adapts its products and systems to the latest developments in cyber security.

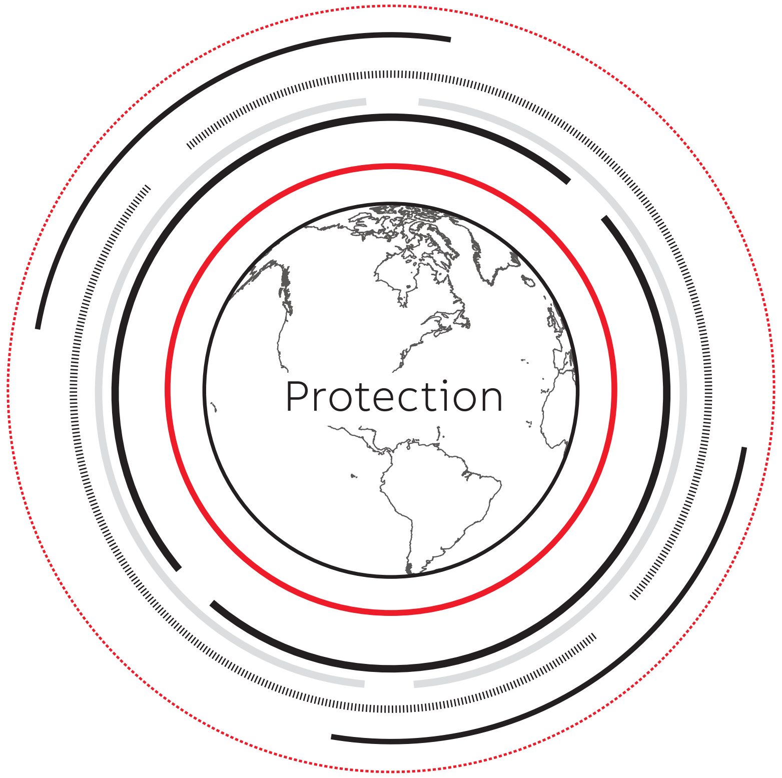
The electric power grid has changed significantly over the past decade and continues to change with technology enhancements. The new generation of protection and control systems are more and more based on open standards and commercial technology, e.g. Ethernet and TCP/IP based communication protocols such as DNP 3.0 or IEC 61850. This change in technology has not only brought huge benefits from an operational point of view, but also introduced cyber security concerns known from office or enterprise IT systems. ABB anticipates the security challenges and constantly adapts its systems to the latest developments in security.

Our Relion 670 and 650 series devices respond to the needs of the power industries and assure a high level of cyber security. User access control, security logging and hardware hardening are implemented according to NERC-CIP and IEEE 1686.

The implemented cyber security functions support users to fulfill the requirements of the BDEW Whitepaper, “Requirements for secure control and telecommunication systems”.

ABB proposes the following cyber security approach:

- Secure system architecture
- Product and system hardening
- Defense in depth approach to address the cyber security challenges
- Service offering to keep the cyber security over the lifetime



User account management

Ease of user management in a network is a standard pre-requisite in today’s digital systems. Relion IEDs enable quick access and cohesive assimilation of user accounts using world class standardized cyber security account management.

User account management

- Audit trail or security logging: The intelligent electronic device enables creation of local user accounts to give the authorized individual the intended rights and log who did what.
- Central account management with IEC 62351 part 8 (LDAP) is a central mechanism to create and maintain users. This functionality is useful to update access for users whose roles change within the company.
- Local replication of user data can be carried out for a specific set of users. This increases reliability and enhances accessibility of your protection and control IEDs.

Role Based Access Control

Relion 670 and 650 series supports Role Based Access Control (RBAC) according to IEC 62351. Every user account can be assigned different roles and the user roles can be added, removed and changed as needed.

Password complexity

Relion 670 and 650 series offers the possibility of enforcing password policies that can be customized by specifying minimum password length, maximum password lifetime, as well as usage of lower case, upper case, numeric and special characters.

Secure communication

IEDs will not allow unauthorized access.

IEDs enable secured communication across the entire grid.

Transport Layer Security (TLS) is used for privacy (to typically conceal passwords) and integrity (to obtain and effect intended IED configurations through the engineering tool, PCM600).

Certificates
- Self signed certificates
- Customer signed certificates
- Encryption of communication

Protocol hardening

Robustness
- All protocols in the IED are checked for conformance
- Fuzz testing is used to make sure we withstand against possible attack points

Secure processes
- ABB's security test center is testing all protocols and interfaces
- All developers follow ABB's security development life cycle process

Only use required surfaces
- To reduce the attack surface of the IED we have added possibility to enable/disable protocols and services per physical interface
- Configure only the services you need

Patch management

Security patches are provided for the 670/650 series. These patches can be implemented without changing the running configuration. This way, vulnerabilities and cyber security findings can be handled in a fast and efficient way. Security patches are included in the maintenance releases together with essential periodic updates.

Logging

The IEDs log and report security events through IEC 61850 and Syslog. The security log is also possible to be retrieved directly from the IED through PCM600.

Supervision and configuration

Supervision of communication
- All communication interfaces are supervised
- Denial of service protection is used to not let flooded interfaces jeopardize the main functionality of the IED, to protect and control the power grid

Configure routes

Relion 670 and 650 series of IEDs allow upto 6 ways for routing traffic from the subnetwork of the IED to another subnetwork.

Efficient infrastructure support for:
- Interstation communication
- Station to station communication
- Station to office communication

Configuration

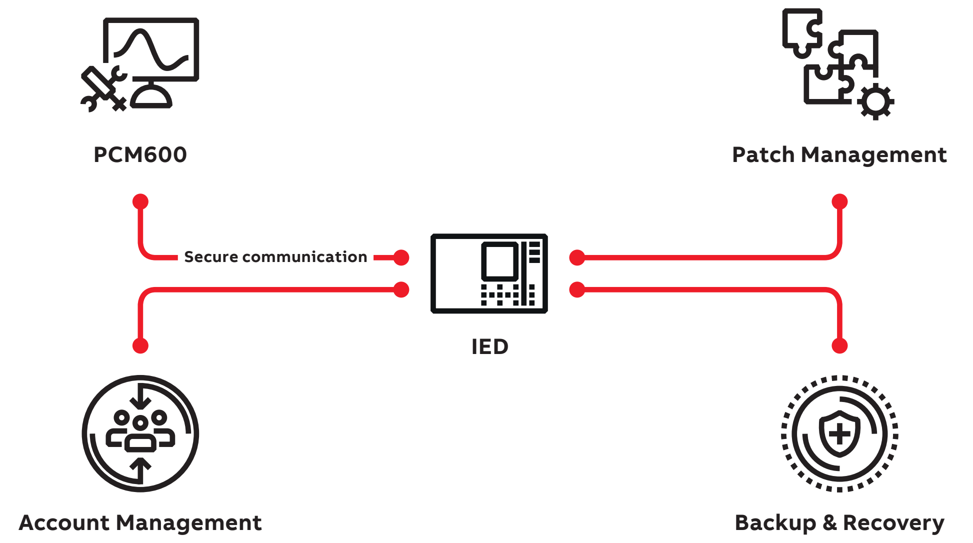
The security configuration is made in PCM600:
- Account management
- Parameter setting
- Ethernet configuration

Trouble shooting

To help the user with common configuration mistakes and to give solutions to common problems, the IED now has a 'hints' menu.

Typical hints can be:
- Incorrect configuration of time synchronization
- Invalid reference channel detected
- IEC/UCA 61850-9-2LE data is substituted

Maintenance is very important to improve the availability of the IED and therefore of the protection and control system. To even further enhance this, the Relion series products now have restore points. A restore point is a way for the user to safeguard their system so that one can always revert back to a previous state. This is very useful prior to applying a new configuration to the IED or before applying a maintenance update of the firmware. The restore point lets the user switch back and forth between the previous state and the new state with just a few manual operations with the IED.



Robustness

ABB strives to improve the security and robustness of its products by performing security testing and hardening. Relion 670/650 series has been systematically hardened, wherein unused services have been removed and unused ports have been closed. Furthermore the 670/650 series has been thoroughly tested at ABB's dedicated, independent security test center using state-of-the-art commercial and open source security testing tools. This includes, first, the detailed documentation of hardening steps and the resulting configurations, for example, open ports and services. While second, security testing and hardening are also integrated parts of the development process.

Traditionally, networks have been isolated and it has taken high fences and barbed wire to keep our critical infrastructure secure.

However, with the increased threat of cyber-attack, governments and industry regulators around the world are focusing beyond physical perimeter protection to ensure the integrity of the systems used to control our power and critical infrastructure.

In a world where technological landscape will be revolutionized by digitalization, a timely response is essential to help customers minimize exposure to cyber security threats.

ABB helps its customers to guarantee long-term security of their data with continually expanding and improving security-related processes to ensure vulnerabilities are handled.

ABB's risk assessment solutions, consulting and training, in addition to technical expertise, provides optimized measures to reduce cyber security risks at the installation.

—

Contact your local service and sales support team to discuss your requirements further.

abb.com/protection-control