Focus on cyber security has steadily increased in the electric sector over the last couple of years. ABB fully understands the importance of cyber security and has identified it as a key requirement.

Our RTUs respond to the needs of the power industries and assure a high level of cyber security. User access control, security logging, hardware hardening are implemented according to NERC-CIP and IEEE 1686. Different algorithms and various encryption standards according to ENISA report are used for all kinds of file storage.

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

**User Account Management**
RTU500 series supports user authentication and authorization on an individual user level. User authentication is required and authorization is enforced for all interactive access to the device.

**User Accounts**
RTU500 series allows to fully manage user accounts, i.e. creating, editing and deleting them freely. User names and passwords can be configured according to customer’s requirements.

**Central Account Management**
RTU500 supports customer owned CAM systems like Windows active directory server. The implementation is based on a LDAP server and complies to IEC 62351-8. Different fall back solutions are available with the RTU500 series in case CAM is not available.

**Secure Communication**

**Web Server**
RTU500 series permits encrypted communication between the web browser and the RTU. A standard browser can be utilized such as Internet Explorer or Firefox. Furthermore the operator can select between https:// and http:// by configuration. In addition, self-signed certificates and customer certificates (X509), can be used.

**VPN Function**
RTU500 series offers an encrypted channel based on the hash algorithms SHA256/384/512 between the RTU and the Psece Router on customers side. The VPN provides confidentiality and integrity and authenticity. A secure communication via public networks is possible. The authenticity is handled by pre-shared keys or customer certifications (X509). A diagnosis interface for encrypted channels is available and can be activated on request for commissioning and troubleshooting. Deactivation of VPN channels in customer networks is not required.

Secure IEC 60870-5-104 Communication (IEC 62351-3)
RTU500 series allows point-to-point data traffic encryption for TCP/IP-based communication. This is enabled thanks to Transport Layer Security (TLS) with respective authentication of client and server using X.509 certificates.

Secure IEC 60870-5-104 Authentication (IEC 62351-5)
RTU500 series prevents “spoofing, modification and replay” of telegrams using IEC 60870-5-104 by adding secure authentication mechanisms. This protocol extension is optimized for low bandwidth consumption and for environments with limited access to authentication servers.

Secure DNP3 Communication (IEC 62351-5)
RTU500 series provides a secure implementation for serial and TCP/IP communication based on DNP3. This part of IEC 62351 focuses on application layer authentication. All application layer messages are defined as critical.

**Integrated Firewall**
RTU500 enables different services on dedicated Ethernet interfaces (E1, E2, USB, PPP). The configuration of the firewall is automatically created from the RTU configuration.

Role Based Access Control
RTU500 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
RTU500 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.

**Manipulation Protection**

RTU installation and RTU documentation are protected by signatures against manipulation. Manipulated RTU download files, e.g. configuration files, are detected and refused.

**Device Supervision via SNMP V3**

Simple Network Management Protocol (SNMP) is one of the most commonly used technologies for network monitoring.

By implementing SNMP, the RTU500 becomes a managed device that can share:
- • Diagnosis information (e.g. CPU load and telegram traffic load)
- • System events (RTU and sub-devices)
- • Configurable Single indications

RTU500 Series can be integrated in Network monitoring systems in parallel to a SCADA system.

**Patch Management**

Security patches provided for the RTU500 series can be implemented without changing the running configuration. This way, vulnerabilities and cyber security findings can be handled in a fast and efficient way, as no release upgrade is required. Patch management is also simplified for large numbers of RTU’s in the project by script interface.

**Security Logging**

**Local Logging**
RTU500 series creates audit trails (log files) of all security relevant user activities. Security events that are being logged include user login, logout, change of parameters, configurations, or updates of firmware. For each event date and time, user, event ID, outcome and source of event are logged. Access to the audit trail is available to authorized users only.

**External Security Clients**
Security events of the RTU can be sent to external security log clients such as the System Data Manager (SDM600). SDM600 is a monitoring and response application, which enables visibility of real time security events. Syslog UDP/TCP and Arcsight TCP - standard protocols for logging of security events - are supported by RTU500 series. Furthermore up to 3 clients per ethernet port can be configured.

**Security Events To Control System**
Security events and alarms can be sent via host protocol to the control systems. “Security indication” and “security alarm” are supported. Settings of security alarms are part of the configuration. Up to 32 security events can be mapped to one single alarm. Security events are available in host protocols, PLC, HMI and process archives.

**Device Supervision via SNMP V3**

Network control center

Firewall

VPN Tunnel

Patch management

User access control

Backup and recovery