Focus on cyber security has steadily increased in the electric sector over the last years. ABB fully understands the importance of cyber security and has identified it as a key focus area. ABB is committed to provide customers with products and systems that clearly address cyber security and thus constantly adapts our products and systems to the latest developments in cyber security.

The electric power grid automation has changed significantly over the past decade and continues to change with technology advancements. The new generation of control systems is more and more based on open standards and commercial technology, e.g. Ethernet and TCP/IP based communication protocols such as IEC 60870-5-104, DNP 3.0 and IEC 61850. This change in technology has brought huge benefits from an operational point of view, but it has also introduced cyber security concerns known from office or enterprise IT systems. ABB anticipates the security challenges and constantly adapts our systems to the latest developments in cyber security.

Our communication and automation system MicroSCADA Pro responds to the need of the utilities and operators and assures a high level of cyber security in order to address requirements of standards and regulations such as NERC-CIP and IEEE 1686.

User access management
MicroSCADA Pro supports user authentication and role-based authorization. User authentication is required and authorization is enforced for all interactive access to the products. Customers can manage user accounts and roles freely, allowing them to create, edit and delete user accounts, and define user names and passwords according to their policies. Usernames and passwords are encrypted and there are no default factory passwords. User accounts can also be managed from a single central location to make the administration easy.

The system also has a configurable time-out feature, which automatically ends user session after a certain amount of time of inactivity or after certain time since the login. There are messages that can be displayed before automatic logout.

Auditability and logging
MicroSCADA Pro creates audit trails (log files) of security relevant user activity. Security events that are being logged include for example user login, logout and password changes. For each event date and time, user, event ID, outcome and source of event are logged. Once a user has logged on, the system keeps track of subsequent user actions.

Secure communication
TCP/IP communication can be secured with VPN solutions that can be achieved with built-in software or by using external hardware such as firewall or router.

Support for virus protection
MicroSCADA Pro systems are protected by virus and host intrusion protection systems. Virus scanner updates and virus definitions are monthly verified in our patch management lab.

Product and system hardening
The robustness of a product can be significantly improved by closing all the ports and services that are not used. MicroSCADA Pro systems are systematically hardened with more strict security policies. For example, unused services are removed and unused
ports closed, and the products are thoroughly tested at ABB’s dedicated, independent security test center using state of the art commercial and open source security testing tools such as Nmap and Nessus. Hardening steps as well as the resulting configurations, such as open ports and services, are documented in detail.

Patch management
The security patches released for the concerned 3rd party products are analyzed regularly. The compatibility with MicroSCADA Pro is analyzed, and in case of risks for incompatibility, system tests are performed to verify the compatibility. In case some problem is found, it is reported in the patch compatibility report, the products concerned are fixed and when the compatibility has been achieved an updated report is published. The compatibility stated in the report means that the security patches can be installed in the system, according to guidelines from the software vendor, without affecting the functionality, stability or performance of the MicroSCADA Pro products.

Documentation
MicroSCADA Pro cyber security deployment guideline collects instructions to harden the system. For example, there is detailed information about port numbers that can be used to configure hardware firewall correctly, or disabling devices (USB ports, CD/DVD drives etc.), which are not used.

For more information please contact:

ABB Oy
Grid Automation Products
P.O. Box 614
FI-65101 Vaasa, Finland
Phone: +358 10 22 11
Fax: +358 10 22 41094
www.abb.com/substationautomation

Note:
We reserve the right to make technical changes or modify the contents of this document without prior notice. With regard to purchase orders, the agreed particulars shall prevail. ABB Oy does not accept any responsibility whatsoever for potential errors or possible lack of information in this document.

We reserve all rights in this document and in the subject matter and illustrations contained therein. Any reproduction, disclosure to third parties or utilization of its contents - in whole or in parts - is forbidden without prior written consent of ABB Oy.

Copyright© 2016 ABB
All rights reserved