1MRS758136 – March 10, 2014

Distribution Automation
NERC-CIP statement concerning Relion® 620 series

Dear Sir/Madame,

ABB fully understands the importance of cyber security for substation automation systems. This document is to demonstrate ABB's commitment to support our customers in their efforts to become or maintain compliance with NERC-CIP requirements.

We have been involved in cyber security for control systems for over a decade and have embedded it as part of our design, development, maintenance, lifecycle management and communications processes. Our activities include e.g. threat modeling and security design reviews, security training of software developers as well as in-house and external security testing.

ABB has chosen a systematic approach to handle cyber security on a global level. We have established a council for power systems and products security to ensure that we have the latest knowledge about the global requirements. The main mandate of the council and its members is to ensure that ABB products and solutions for power systems meet the expectations of our customers and are compliant with industry standards and regulations on cyber security, such as NERC-CIP. The council is also responsible for ensuring active ABB involvement in national and international security efforts.

ABB strives to continuously improve the security and robustness of its products. Therefore, ABB has integrated security testing as a mandatory part of the product development process. A dedicated, independent security test centre has been established where ABB products are subject to security and robustness tests. The tests utilize current state-of-the-art commercial and open source security testing tools. The security tests include profiling, known vulnerability, denial of service and negative protocol tests.

About the NERC-CIP standard

The Critical Infrastructure Protection (CIP) standards developed by the North American Electric Reliability Corp. (NERC-CIP) are performance based standards, and thus only power utilities and other end-users can be NERC-CIP compliant. Systems, subsystems or products sold or delivered by ABB or other suppliers cannot be NERC-CIP compliant as such. They can, however, include technical features that support the utilities or end-users to be NERC-CIP compliant. ABB is committed to support the end-users in their compliance efforts, and thus ABB provides the information included in this document. The compliance to NERC-CIP, however, is ultimately the responsibility of the end-user.

The following information provides an overview of the cyber security features included in the Relion 620 series IEDs according to NERC-CIP standard.

ABB Oy
Medium Voltage Products
FI-65101 Vaasa, Finland
Tel. +358 10 22 11
Fax. +358 10 22 41 094
www.abb.com/substationautomation

1MRS758136 – March 10, 2014

Distribution Automation
NERC-CIP statement concerning Relion® 620 series

Relion® 620 series cyber security features

Authentication, authorization and user management
The 620 series supports role based user authentication and authorization. The user authentication and authorization are configurable for creating access rights to the products. The power utilities and end-users can freely manage user authorization passwords.

The user passwords can be up to 20 characters. The passwords are case sensitive and support alphanumeric characters and non-alphanumeric characters.

Malicious software prevention
The 620 series products are using an embedded operating system. Products based on such operating systems do not support installation and execution of non-ABB scripts and software. The probability of encountering malicious software attack is extremely low. However, ABB regularly performs stress and vulnerability scanning tests on its 620 series protection and control IEDs to ensure the robustness of the products.

Auditability & Logging
All operational events and user activities are logged in the IED's event list. Such events are e.g. breaker control, protection activation, configuration change, time synchronization and internal supervision data. The event list is read-only data and the data is stored to a non-volatile memory.

Security testing and product hardening
The 620 series has been tested in our independent robustness test centre. Only ports and services which are needed for normal operation are enabled. By default other ports and services are disabled.

The electric power grid has been evolving significantly over the past decade. This process incorporates present and future technology development. ABB has identified cyber security as a key requirement for reliable operation of power systems and is committed to provide customers with products, systems and services that clearly address cyber security.

Yours faithfully,

Markus Kortesluoma
Global Product Manager
Protection and control products
Distribution Automation

Janne Starck
Product Line Manager
Protection and control products
Distribution Automation

ABB Oy
Medium Voltage Products
FI-65101 Vaasa, Finland
Tel. +358 10 22 11
Fax. +358 10 22 41 094
www.abb.com/substationautomation