Dear Reader,

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 achieve or maintain compliance with Qatar’s National ICS Security Standard 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. Examples of activities include threat modelling 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 Power Grid Security Council to ensure that we have the latest knowledge about the global requirements. The 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 and supporting industry standards and regulations on cyber security, such as Qatar’s National ICS Security Standard. 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 and has integrated security testing as part of the development process. A dedicated, independent security test centre has been established where ABB products are subject to security and robustness tests utilizing current state-of-the-art commercial and open source security testing tools. Tests include profiling, known vulnerability, denial of service and negative protocol tests.

About Qatar’s National ICS Security Standard
Qatar’s National ICS Security Standard v.3-March 2014 is a performance based standard and, thus, only utilities and other end-users can be National ICS Security Standard compliant. Any system, subsystem or product sold or delivered by ABB or other suppliers cannot be National ICS Security Standard compliant. They can, however, include technical features that help support utilities or other end-users in becoming National ICS Security Standard compliant. ABB is committed to supporting end-users in their compliance efforts, and thus provides the information included in this document. Compliance to National ICS Security Standard, however, is ultimately the responsibility of the end-user.

The following information provides an overview of the cyber security features included in the MicroSCADA Pro products SYS600, SYS600C and DMS600 according to National ICS Security Standard.
MicroSCADA Pro cyber security features

Authentication, authorization and user management
MicroSCADA Pro products support role based user authentication and authorization. User authentication is required and authorization is enforced for all interactive access to the products. Utilities and end-users can manage user accounts freely concerning creating, editing and deleting user accounts, as well as freely choosing usernames and passwords.

User passwords are encrypted using industry standard methods, can contain up to 32 characters, and passwords are case sensitive and support alphanumerical characters and non-alphanumerical characters. The products also support password policies that allow customers to specify minimum password length and password complexities.

Malicious software prevention
The MicroSCADA Pro products run on standard Microsoft Windows operating systems and state-of-the-art security solutions, such as anti-virus protection, firewalls, intrusion protection can be deployed. ABB also regularly performs stress and vulnerability scanning tests on MicroSCADA Pro products to ensure the robustness.

Patch management
MicroSCADA Pro is regularly tested every month to verify compatibility with security patches for operating systems, virus protection software and other related software that is used together with the products. This ensures that the systems can be kept up-to-date and thereby be protected in the best possible way.

Auditability & Logging
MicroSCADA Pro logs both user session related events, such as logon/logoff and operational events, such as breaker control. All events are protected by access control mechanisms.

Security testing and product hardening
The MicroSCADA Pro products have been tested in our independent robustness test centre in order to ensure in depth security of the products. Only ports and services which are needed for normal operation can be enabled and other ports and services can be closed.

The electric power grid has evolved significantly over the past decade and continues to do so along with technology advancements. ABB has identified cyber security as a key requirement and has committed to provide customers with products, systems and services that clearly address this.

Yours faithfully,

Frank Hohlbaum
Global Security Manager
Grid Automation

Mikael Molander
Global Product Manager, MicroSCADA Pro
Grid Automation Products

NOTICE
The information in this document is subject to change without notice. In no event shall ABB be liable for direct, indirect, special, incidental or consequential damages of any nature or kind arising from the use of this document, nor shall ABB be liable for incidental or consequential damages arising from use of any software or hardware described in this document.

ABB
Grid Automation Products
FI-65100 Vaasa, Finland
Tel. +358 10 2211
Fax +358 10 2241599
www.abb.com/substationautomation