STUDY OF INTERNATIONALLY ACCEPTED CYBER SECURITY STANDARDS AND THEIR IMPLEMENTATION TO STATION LEVEL DEVICES

by

Imran Ali Rizvi, B.Sc. Electrical Engineer,1990, UET Lahore Pakistan

A project
presented to the Ryerson University
in partial fulfillment of the
the requirements for the degree of
Master of Engineering
in the Program of
Electrical and Computer Engineering

Toronto, Ontario, Canada, 2014

Author's Declaration for Electronic Submission of a Project

I hereby declare that I am the sole author of this project. This is a true copy of the project, including any required final revisions, as accepted by my examiners.

I authorize the Ryerson University to lend this project to other institutions or individuals for the purpose of scholarly research.

I further authorize the Ryerson University to reproduce this project by photocopying or by other means, in total or in part, at the request of other institutions or individuals for the purpose of scholarly research.

I understand that my project may be made electronically available to the public.

Abstract

Title of Project: Study of Internationally Accepted Cyber Security Standards and Their Implementation to Station Level Devices
Degree: Master of Engineering Degree in Electrical and Computer Engineering
Year of Convocation: 2014
Full Name: Imran Ali Rizvi
Ryerson University

The convergence of electric power grid with the IP-based communication network has posed many security threats to sustained power supply demands of our ever growing power system. A lot of work is required to find out innovative security solutions for smart grids which meet the stringent requirements of power network but at the same time provide security to the flow of information between the embedded IEDs in the power system.

The project will first cover an in depth study of these standards/ guidelines and, security techniques.

In the second part of the project, we will examine the implementation of these standards and guidelines on the station level devices like numerical relays, from renowned manufactures. A setup in the lab with a numerical relay and associated software tool will be made, to practically demonstrate the cyber security configurations in a real life situation in a substation.

Acknowledgements

I would like to express my special appreciation and thanks to my supervisor Professor Dr. KAAMRAN RAAHEMIFAR, you have been a tremendous mentor for me. I would like to thank you for encouraging my research and for allowing me to grow as a professional engineer. Your advice on both research as well as on my career have been priceless. I also want to thank you for letting my defense be an enjoyable moment, and for your brilliant comments and suggestions, thanks to you.

A special thanks to my family. Words cannot express how grateful I am to my wife, and kids for all of the sacrifices that you’ve made on my behalf. Your prayer for me was what sustained me thus far. I would also like to thank all of my friends who supported me in writing, and incented me to strive towards my goal.

Dedication

I dedicate my dissertation to my family and many friends who have been very helpful in achieving this goal.

Table of Contents

Contents

List of Tables

List of Figures

List of Appendices

Chapter 1: Introduction

The electric power grid has evolved significantly over the past decade thanks to many technological advancements and breakthroughs. As a result, the emerging “smart grid” is quickly becoming a reality. At the heart of these intelligent advancements are specialized IT systems – various control and automation solutions such as substation automation systems. To provide end users with comprehensive real-time information, enabling higher reliability and greater control, automation systems have become ever more interconnected.

The new generation of automation systems uses open standards such as IEC 60870-5-104, DNP 3.0 and IEC 61850 and commercial technologies, in particular Ethernet- and TCP/IP-based communication protocols. They also enable connectivity to external networks, such as office intranet systems and the Internet. These changes in technology, including the adoption of open IT standards, have brought huge benefits from an operational perspective, but they have also introduced cyber security concerns previously known only to office or enterprise IT systems.

To counter cyber security risks, open IT standards are equipped with cyber security mechanisms. These mechanisms, developed in a large number of enterprise environments, are proven technologies. They enable the design, development and continual improvement of cyber security solutions specifically for control systems, including substation automation applications.

1.1 Background

Over time words tend to change meaning as culture and perceptions change and new ideologies are adapted. The word “security” has in the past conjured up images of comfort, the physical protection offered by family and friends, stable financial prospects, and peace of mind. However in recent years our image of the word security has changed into something more likely to do with locks and gates, portable alarm devices, missile defense systems, and space shields. Change has also occurred in terms of the use of the word with respect to the area of computers - what is commonly known as cyber security. Security was not an issue of concern when computers were in their infancy and the Internet’s predecessor, ARPANET, was developed for use by the scientific and academic community. However computers are no longer the technical amusement of a select group with trusted network access to any and all, but are now a commonplace and integral part of everyday life in our society and, unfortunately, now subject to frequent malicious attacks and electronic vandalism.

Initially when computers became networked electronic information in the form of data and applications was commonly exchanged via the use of FTP, or file transfer protocol. A user could typically log into a computer site using their email address and the password “anonymous” and be greeted with a “welcome” message. The guest would then have easy access to desired information, including oftentimes system files. Soon this technology became subversively exploited and the industry was told not to expect to prosecute violators when an open door and a welcome mat were laid out for common use. Security gradually took on a new meaning as the hosts of computer data sites became increasingly aware of issues surrounding the vulnerability and protection of their information and networks. Today it is not uncommon to have networked computer sites visited and attacked on a regular basis (1000’s of times per day) by subversive forces for reasons ranging from espionage, extortion, “cyber protests”, revenge, and sport. Not only are computer sites vulnerable to direct and focused attack, but they are also vulnerable to indirect, or indiscriminate, attacks from viruses, worms and Trojan horses.

As technology has increased, the use of computers and network access has also increased. Computers, or microprocessor-based devices with computing capability, are now commonly used for control and automation functions in addition to traditional data archival and processing. Computers preside over a plethora of daily activities from financial, manufacturing, scientific, and safety-rated issues. Millions of computers are connected to the Internet and now form a vast interconnection of devices used by corporations, individual, and government agencies. As can be imagined with this convenient and widespread use, the opportunity for misuse has also burgeoned.

Technological misuse and/or abuse has become a serious concern in all areas where computers are used and networked. The ability of seditious individuals to disrupt the national power supply, discharge harmful chemicals or waste into the environment, or upset production facilities, has become an unwelcome verity. Not only are there financial and safety concerns associated with this, but also issues relating to legal liability where individuals or corporations can be sued for mismanagement of technological resources. Other issues arising from compromised computing facilities are loss of customer confidence, information confidentiality, and the ability to conduct business. Computer security has now become the focus of national consideration.

The electric power industry, as the rest of society, has been taking advantage of the tremendous power provided by computer and microprocessor-based technology. Fig 1.1 shows the typical communication network used for smart grids. Protection and control equipment, SCADA, remote control and monitoring, and many other applications are routinely implemented with this technology. Recent experience has shown that security related issues must be addressed by the power industry. Government regulation will soon legislate the need for proactive measures to be taken in terms of securing the computer network infrastructure within the power grid. The electrical supply is too important to be left in a state of vulnerability and neglect.

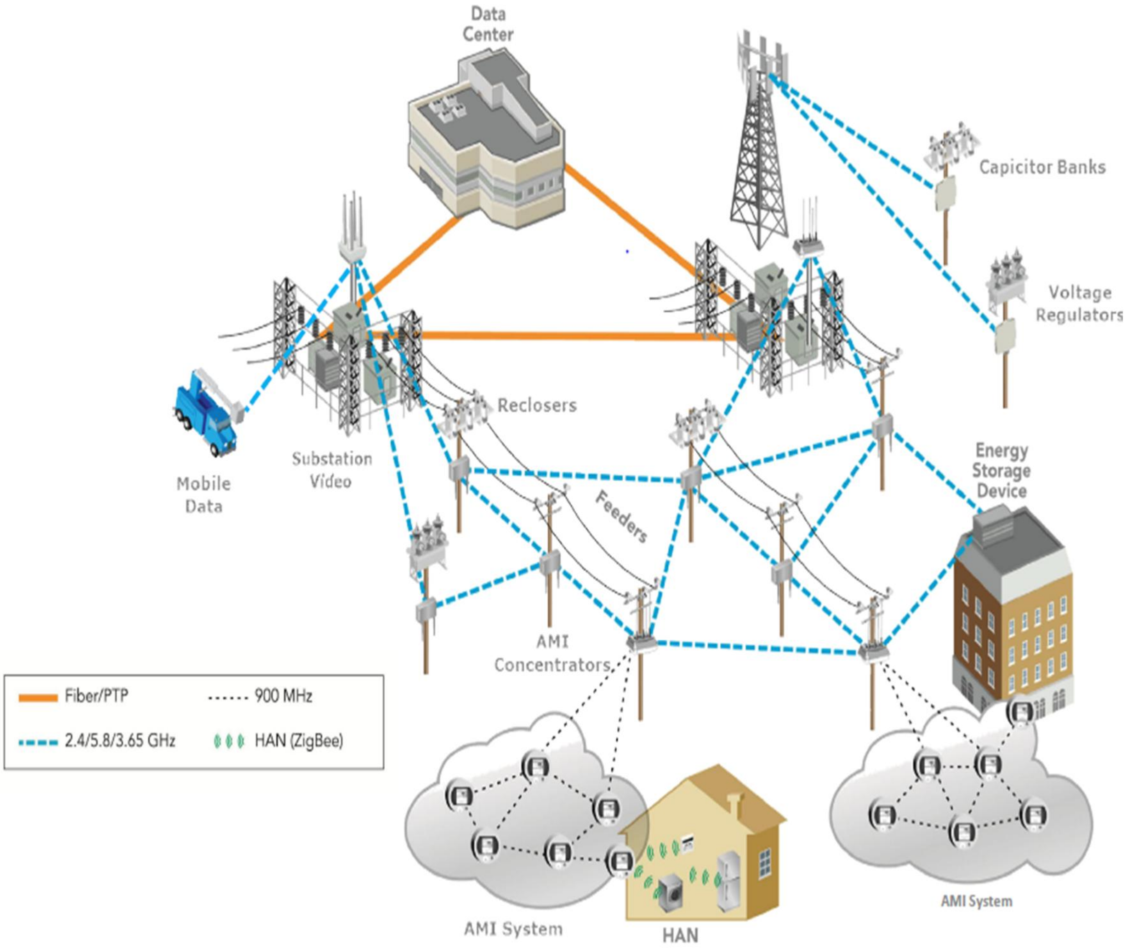


Fig 1.1. Communication Network for Smart Grid

1.2 Data Access Needs for Protection Engineers

Utility personnel require remote access to the protection, control, and monitoring devices located in substations scattered throughout the system. This access is required to: continuously assess the health of the system; recognize developing problems that may adversely affect the ability of the system to remain operational; identify the location of faults and failures to facilitate the dispatch of repair crews; analyze the operation of protective devices to ensure correctness and maintain coordination to prevent cascading outages; identify possible improvements to protective schemes; verify the accuracy of system models to facilitate planning studies. Some of the devices for which access is needed are:

- Microprocessor-based protective relays
- Digital fault recorders
- Dynamic disturbance monitors
- Phasor measurement units
- Power system stabilizers
- Geo-magnetically-induced current monitors
- Remote terminal units (RTU) of system control and data acquisition (SCADA) systems
- Substation Computers
- Data Historians
- SCADA systems
- Security systems (fire, intrusion, etc.)

The level of access required depends on job function. System control operators need to know what happened and where (breaker status changes, system element loading, relay target data and fault locations, intrusion alarms, etc.)

Protection engineers typically need to read the stored data (relay, fault recorder, and disturbance monitor event records and setting records) in order to analyze system disturbances, support operations personnel, coordinate protection schemes, and ensure compliance with NERC standards. Protection Engineers can also make settings changes as required due to changes in system configuration. Field relay technicians need read/write access to all levels of the devices in order to apply the settings determined by the protection engineers and set up the devices for proper operation and communication with those that need access.

Access needs to be available within the substation and corporate offices. Fig 1.2 shows a typical substation automation system. A limited number of personnel will require full access at non-company locations. The expectation of round the clock analysis capabilities and the quantity of data available often requires access via the Internet. A dial up connection may also be used for less demanding requirements. Access to the corporate “Data” network via the Internet raises the highest level of concern for cyber security.

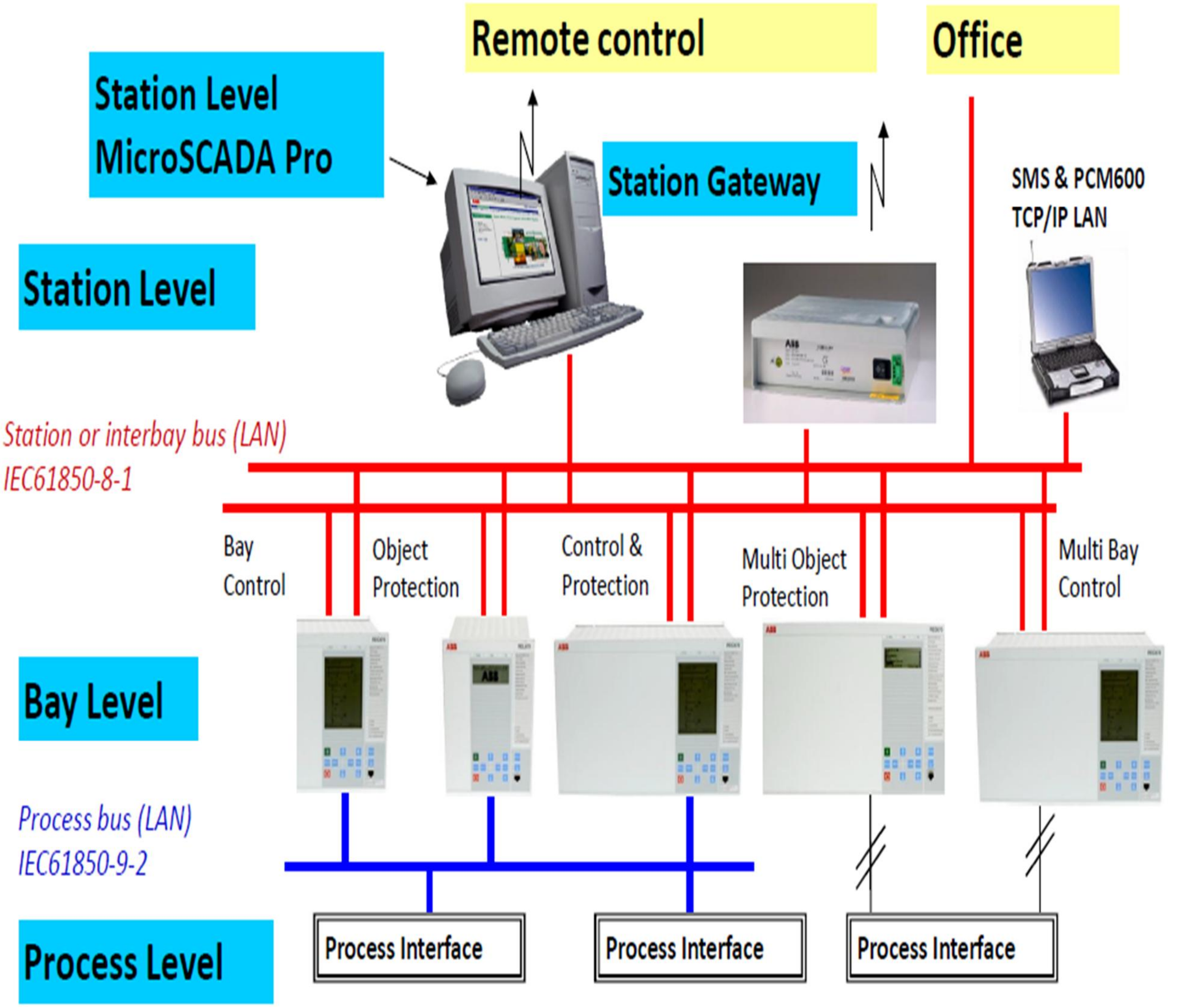


Fig 1.2. Typical Substation Automation System

1.2.1 Relay Access and Settings Considerations

Relays are critical to the power system. The settings in a relay determines the response (or non-response) of the device and incorrect settings may have serious effect on the power system operation.

Typically, relay settings are allowed to be changed by Protection Personnel only, but the multi-function nature of microprocessor relays have extended use of protection devices to other groups as well. A modern relay may replace a traditional RTU and provide metering data and control functions for opening and closing breakers and other switches. A relay may also be connected to a substation computer that performs automation and control functions. The multi-function nature of the relay device may generate the need to extend ‘setting-change-privileges’ to others than protection engineers which creates an added challenge for the protection engineer to track, document and verify relay settings. Modern relay designs recognize the need for increased access to the device and provide some means to help the relay engineer with regards to setting changes. Some examples are:

- Passwords. Most relays have the ability of password protection for settings changes.
- A relay log for setting changes, and to issue an alarm when a setting change has been made.
- Multiple levels of access, with different passwords for each level. Typically, there is a read-only level that may be accessed by a larger number of users while the higher level for setting changes can be accessed by the relay engineer only.
- A relay with multiple settings groups where a switch to another per-verified group may be allowed by non-relay personnel, while change of individual parameters is not.

While procedures for access restriction to the substation are well established, the increased remote access to microprocessor relays is less regulated.

Typically, a utility utilizes the extended capability of microprocessor relays to provide status, control and metering functions to a station RTU via a serial communication link. This functionality has replaced traditional analog transducer and hard-wired alarm connections to a central station RTU in all new installations and many retrofit locations. Any settings required for these extended functions should be communicated to the protection engineer during the schematic and/or relay setting development phase. The automation engineer may also initiate setting changes through the protection engineer if only changes associated with automation are required. Ultimately, the protection engineer should be the individual responsible for all protective relay settings and documentation – the automation engineer works through the protection engineer to implement necessary automation settings.

Preferably, relay access passwords should be established that allow view-only user access to automation engineers (and maintenance personnel, system operators…). A second, more secure level in which setting changes may be made should be reserved for relay engineers and test technicians. Testing contractors may utilize temporary passwords to complete necessary setting changes and testing.

Relays have settings that can be generally grouped into the following categories: protection, communication (usually related to integration and automation, not teleprotection), and security. Utilities may have processes in place that dictate if any relay setting has changed, including the communication and security settings, the relay must be re-commissioned. This re-commissioning policy can be beneficial when relay communication settings are changed. With the deployment of protective relays on substation LANs using IEC 61850, it is possible that communication settings could be changed (such as IP address) that would adversely impact the protective functions of the relay.

This re-commissioning policy may adversely impact the procedures put in place for securing relays, where relay passwords must be changed under certain situations (employee leaving, contractors leaving, password aging, etc). In these situations where relay passwords must be changed, requiring a re-commissioning of all relays where the password(s) are changed can quickly become impractical because there may be hundreds or thousands of passwords to change, and in some cases, re-programming of devices that include passwords in the retrieval of SCADA data from relays.

.

Relay re-commissioning after a settings change should include a careful review of how communication and security settings impact overall device integration and security policies. This review should include not only relay engineers, but automation engineers and security professionals as well. For example, relays that do not perform protective functions over a LAN and are polled using DNP over the LAN may only require a quick point check to confirm that polling has been re-established after a communication settings change; relays that do not perform protective functions over a LAN and are polled using DNP do not require re-commissioning after a password change. It is possible that the relay setting change process may drive the technological solution for the security process, or vice-versa.

1.3 Communication Media

There is a large variety of communications routes for access of devices in substations. The physical media can be Point-to-Point (telephone lines), Microwave, and higher bandwidth transport (T1, SONET or Ethernet).

A. Typical Point-to-Point Communications Media

- POTS (Plain Old Telephone Service) dial-up via phone line – The most common medium used to access relays remotely is dial-up phone lines. A standard voice line run into the substation provides the path. Modems are required to interface the phone line with the IED RET650s. Line switchers typically allow one phone line to be switched and used for relay access, meter access, phone conversations, etc.
- Leased line – Leased lines are typically used for SCADA connection. They are dedicated lines that are connected 24 hours a day, 7 days a week. They allow constant data acquisition and control capability of substation equipment.
- Wire-less – Wire-less communication (cellular phones) is a technology that is useful in the substation environment. It can be less expensive than a hard phone line due to the protection required by Telcos on a phone line run into a substation to limit ground potential rise. The cost is based on actual usage (minutes used). Usability may be limited by cellular coverage in the area but that is continually improving.
- Radio – 900 MHz radio is another medium used by utilities. These radios can either be licensed or unlicensed depending on the frequency selected. The unlicensed installations have a lower installed cost but there is no protection from interference by other users.

B. Microwave

Microwave is a high frequency radio signal that is transmitted though the atmosphere. Common frequency bands are 2 GHz, 4 GHz, 6 GHz, 10 GHz, 18 GHz, and 23 GHz. Transmitted signals at these frequencies require a direct line of site path, and accurate antenna alignment. The federal Communications Commission (FCC Parts 21, and 94) controls operation and frequency allocations.

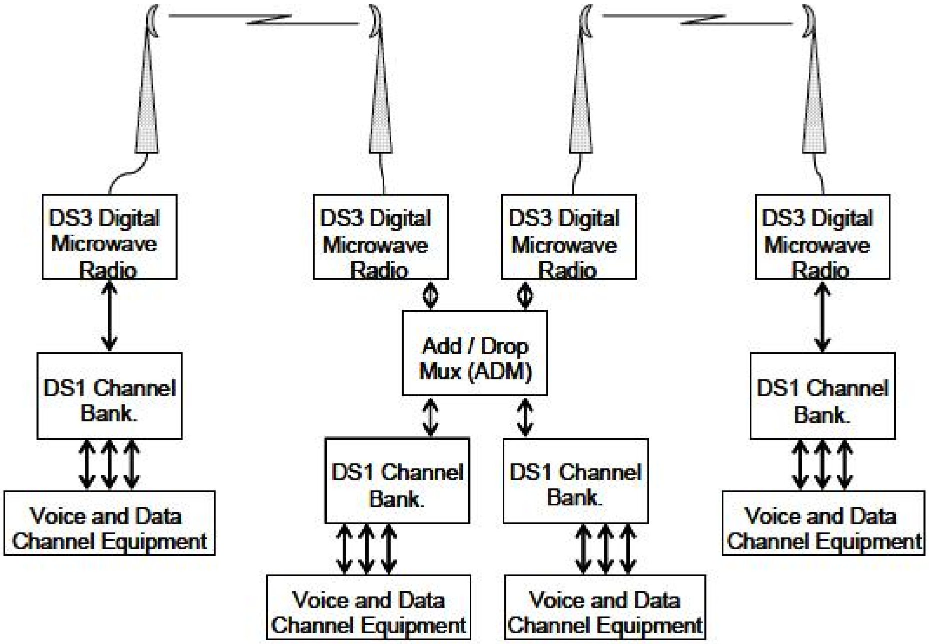

DS3 Digital Microwave Radio
DS3 Digital Microwave Radio
DS3 Digital Microwave Radio
DS3 Digital Microwave Radio
Add / Drop Mux (ADM)
DS1 Channel Bank.
DS1 Channel Bank.
DS1 Channel Bank.
DS1 Channel Bank.
Voice and Data Channel Equipment
Voice and Data Channel Equipment
Voice and Data Channel Equipment
Voice and Data Channel Equipment

Fig 1.3. Typical Microwave System

In digital microwave systems the data modems, required in an analog system, are replaced by digital channel banks. These channel banks can be combined to form a multiplexed system as shown in Figure 1.3. The channel banks convert analog voice, and data inputs into a digital format using Pulse Code Modulation (PCM). The digital channel bank combines 24 voice channels into a standard 1.544 Mbps DS-1 signal. The DS-1 level is further multiplexed into DS-3 before transmitted over the radio link.

C. T1, SONET and Ethernet Transport Layer

Many substations are served by T1, SONET or Ethernet access equipment to provide a communications path to the substation device. T1 is a term for a digital carrier facility used to transmit a DS-1 formatted digital signal at 1.544 megabits per second.

T1 was developed by AT&T in 1957 and implemented in the early 1960's to support long-haul pulse-code modulation (PCM) voice transmission. The primary innovation of T1 was to introduce "digitized" voice and to create a network fully capable of digitally representing what was, up until then, a fully analog telephone system.

T1 is used for a wide variety of voice and data applications. They are embedded in the network distribution architecture as a convenient means of reducing cable pair counts by carrying 24 voice channels in one 4-wire circuit. T1 multiplexers today are also used to provide DS0 "access" to higher order 'transport' multiplexers such as 'SONET'.

SONET (Synchronous Optical NETwork) is the American National Standards standard for synchronous data transmission on optical media, shown in Fig 1.4.

Some of the most common SONET (and SDH) applications include transport for all voice services, internet access, frame relay access, ATM transport, cellular/PCS cell site transport, inter-office trunking, private backbone networks, metropolitan area networks and more. SONET operates today as the backbone for most, if not all, interoffice trunking as well as trans-national, and trans-continental communications.

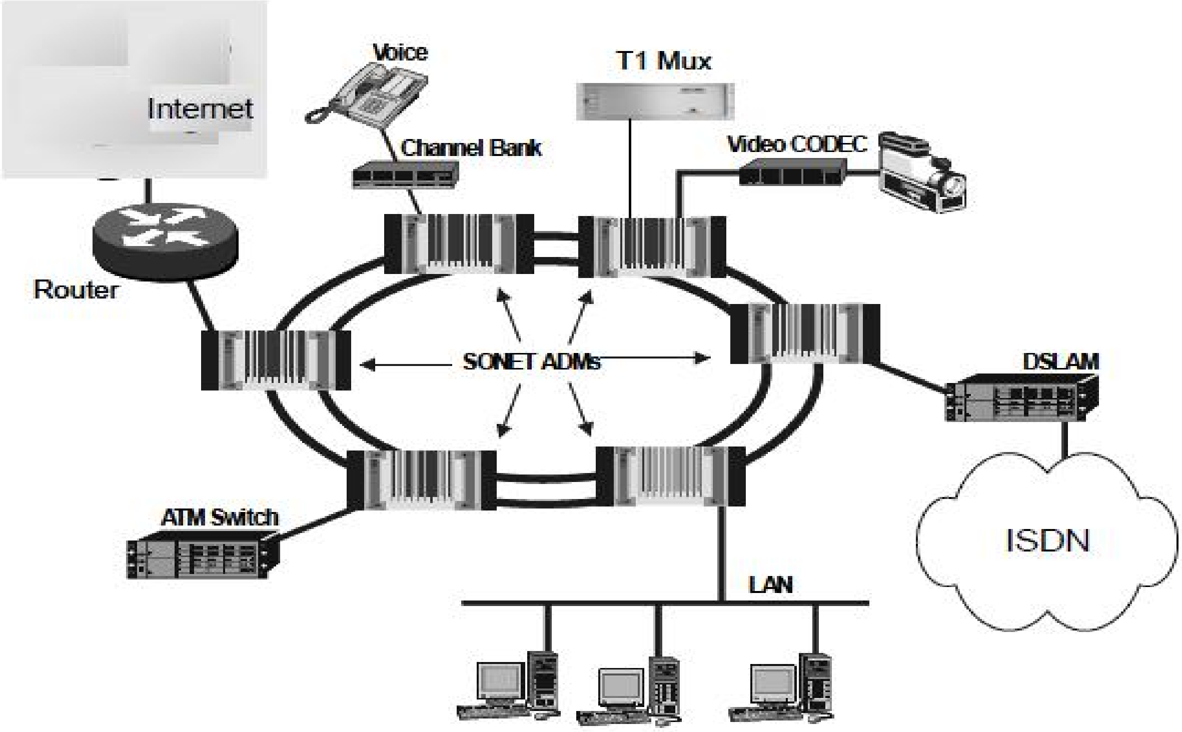


Fig 1.4. SONET System

IP Communications (Ethernet) is growing as a substation access technology. The transport is often over a SONET layer, but Ethernet LANs are also used.

The communications network can be privately owned by the utility, or leased from a carrier. A Local Area Network (LAN) can have its own dedicated communications links or exist as a VLAN (virtual local area network) where the transport layer is shared with other, unrelated traffic.

The LAN or VLAN may interconnect with a Wide Area Network (WAN) that carries corporate traffic and/or is a public transportation network.

D. Communications Media Cyber Security Concerns

Electronic eavesdropping can be achieved in all communications media by intercepting or tapping into communication signals. Dial-up phone lines are especially vulnerable as the device connected to it can be directly accessed through the public telephone network. Any security needs to be handled by the device itself. Leased phone lines are more likely to suffer from denial of service rather than interception due to the highly specialized and often proprietary data they carry.

Eavesdropping in Local Area Networks (LAN) and Wide Area Networks (WAN) is called sniffing. A sniffer is a program that accepts and opens network packets that are not addressed to your equipment.

Wireless eavesdropping and sniffing can occur on virtually all commonly used wireless networks including, radio, satellite, and microwave transmissions.

1.4 Communication Systems

Communication to the substation device can be point-to point, over a Local Area Network (LAN), Virtual Local Area Network (VLAN), or Wide Area Network (WAN). The type of communications system is not directly related to the communication media as various media can be deployed within one network.

1.4.1 Internet

Technologies have been developed that allow Internet access to substation devices. Each device is assigned a unique Internet address and is connected to a LAN in the substation and on to the Internet. Web browser software can be used to communicate with the devices.

Cyber Security in the Substation can be addressed at both the Data link and Network layers of the OSI model. The addressing mechanism at the Data link layer is the Mac address which is predefined by the manufacturer of the Ethernet enabled communications equipment. At the Network Layer the IP address is used.

The network should be secured at both layers. Each communications device used on the network has specific vulnerabilities and in most cases features to deal with them.

Many of these features need to be configured. Security design within the network is paramount in the process of securing the network. While securing the network the following features should be considered.

1) Security at the Data Link Layer

The Data link layer is commonly called layer 2. At this layer switches are the most prevalent communications equipment used. Many different features are available on the switches that can impact the Security on the network.

2) Management Security

Switches have their own security to protect against intrusion or unauthorized configuration. Switches should be configured with passwords and secrets which are unique and follow strong password standards. SSL or SSH should be used when configuring switches to prevent sniffing these passwords.

3) Port Security

Individual ports on the switch can be secured using several methods. In the simplest form they may be enabled or disabled. It is recommended unused ports be disabled. Each port may be further secured using MAC based security, 802.1x or VLAN filtering.

4) MAC Security

When MAC based security is used each port on the switch can be configured to allow communications only from one specific MAC address. With this method of security, only the IED RET650's intended to communicate on any given port (or a hacker spoofing an IED RET650’s MAC address) can do so.

5) 802.1x

With this technology devices are forced to authenticate with a predefined user name / password before they gain access to the network. 802.1x clients are required on the IED RET650 in order to make this effective. Most windows clients available today have integrated 802.1x clients. The authentication is usually done by a third party entity, such as a RADIUS server.

6) VLAN Security

When VLAN based security is used, all traffic entering thenetwork comprises (or is assigned) IEEE 802.1Q “tagged” frames, with each tag’s “VID” field identifying a specific VLAN. Un-trusted sources are assigned (on ingress) an appropriate VID to guarantee the isolation of such sources from the traffic assigned to other VID’s.

1.4.2 Security at the Network Layer

The Network layer is commonly called Layer 3. At the Network layer many devices can be used to secure the network. The devices commonly used at this layer are Routers, Firewalls and Intrusion detection devices. Some Security appliances are available that offer all three functions in one box.

1) Management Security

Routers / Firewalls / Intrusion detection devices have their own security to protect against intrusion or unauthorized configuration. These devices should be configured with passwords and secrets which are unique and follow strong password standards. SSL or SSH should be used when configuring these devices to prevent sniffing these passwords.

2) IP Filtering

Filtering can be done by Routers and Firewalls. Filtering can be used to deny access to the Substation network from unauthorized IP networks. In order to use this feature effectively the IP address space within the entire Utility should be assigned effectively.

3) Port / Socket Filtering

Filtering can be done at the Port / Socket layer. Ports/Sockets are used to identify traffic by type. These can be services such as FTP, HTTP or Telnet. Many organizations prohibit some of these services on the Substation LAN by policy.

4) Anomaly Detection

Intrusion Detection devices can be used to look for network anomalies. This is done by comparing traffic against a known database of signatures which identify traffic patterns which are known to present network vulnerabilities. When an anomaly is detected on the network the network administrator is notifIED RET650. The network administrator will generally take action by configuring filters on the Routers or Firewalls.

5) Encryption

Encryption can be used on the LAN to secure traffic against unauthorized access. This can be done for Routers, Firewalls and some IEDs. Several different types of Encryption algorithms are commonly available. These include DES, 3DES or AES. 3DES is the most common. AES is a newer standard which offers a higher level of security.

1.5 Relay Pilot Channels

Pilot protection schemes and SCADA control schemes are similar in that either system can potentially initiate breaker tripping. The communications channels and equipment requirements for pilot protection schemes differ from those used for SCADA in the following ways:

- They are predominantly operated on private, closed, and deterministic networks.

- Signal transmission and reception must have known and minimal delays.
- With the exception of direct transfer trip schemes, most pilot protection schemes qualify received messages with locally measured quantities.

The most widely used pilot protection system is directional comparison. Major reasons for this wide acceptance are the low channel requirements (i.e., lower data rate, small message sizes, etc.) and the inherent redundancy and backup of directional comparison systems. Although the channel bandwidth requirements are less than those of current differential schemes, the communication channel data integrity requirements are significant. We may classify directional comparison pilot protection systems as blocking or transfer trip. This classification corresponds to the way the local relay uses remote terminal information to generate the tripping signal.

A current differential system is another popular pilot protection scheme. Such schemes compare the magnitude and/or phase of the currents from all terminals. This means that current differential schemes require a reliable, high capacity communications channel. When communication fails, the differential protection portion of these schemes must be blocked from operating. Today, many current differential schemes use redundant communications to handle the loss of a single channel.

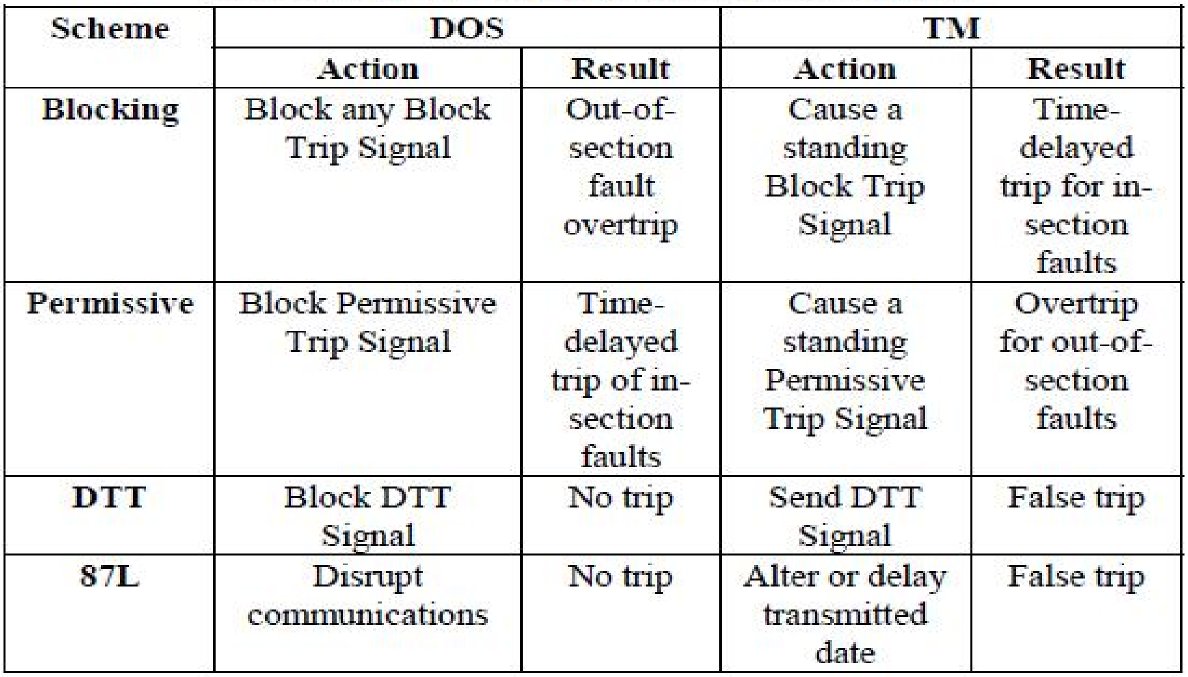
All pilot schemes are characterized by the need for a reliable communications channel between the line-end devices. It is not necessary to extend or network the connections to any other devices. In practice, the majority of these communications channels are deployed on wholly owned (i.e., not leased from a telecomm provider) media such as fiber or the power line itself. Because of this, most real time protection communications have very limited exposure to potential electronic attack.

Assuming that attackers are able to access the communications media (either electronically or physically), they could potentially execute the following general attacks:

- Denial of Service (DOS): Cause a break in the normal transmission of real-time protection messages.
- Traffic Manipulation (TM): Intercept legitimate traffic and/or inject malicious traffic on the line.

The effect of a DOS or TM attack depends upon the type of protection scheme. Table I shows the action and results for the various schemes.

TABLE I – EFFECT OF ATTACK ON PILOT RELAYING



Scheme	DOS		TM	
	Action	Result	Action	Result
Blocking	Block any Block Trip Signal	Out-of-section fault overtrip	Cause a standing Block Trip Signal	Time-delayed trip for in-section faults
Permissive	Block Permissive Trip Signal	Time-delayed trip of in-section faults	Cause a standing Permissive Trip Signal	Overtrip for out-of-section faults
DTT	Block DTT Signal	No trip	Send DTT Signal	False trip
87L	Disrupt communications	No trip	Alter or delay transmitted date	False trip

The blocking and permissive trip protection schemes provide high immunity to any potential attack damage (it is simply not possible to cause a severe mis-operation through manipulation of the communications channel). For the direct transfer trip (DTT) scheme, we can eliminate the possibility of tripping the local breaker with local supervision. Examples of local supervision are overcurrent, under voltage, power, and rate-of-change elements. Finally, for current differential (87L) protection schemes, you can eliminate the loss of line protection resulting from channel failure (either accidental or deliberate) with effective backup communications and protection schemes.

Current differential schemes are extremely dependent upon communications: a DOS attack on a line current differential scheme does disable the primary, 87L protection on the line. However, many schemes include true hot-standby 87L communications and directional comparison protective schemes in the same device. Thus, in the event of an attack, the complete scheme would disable one of the 87L schemes and alarm, yet line protection would remain intact. It is possible, however, to initiate a false trip for DTT (without supervision) and 87L protection schemes with a TM attack. This may not be a cause for concern because of the limited exposure of most real-time protection communications.

The limited risks outlined above may warrant additional electronic security if the communications channels used to implement pilot protection schemes are not “sufficiently” secure. Such a decision can only be made by weighing the potential costs of an inadvertent breaker trip versus the risk of electronic attack.

1.6 Reasons for Security

A number of issues are of serious concern with respect to power system security. In a society where companies and individuals increasingly succumb to litigation for reasons of negligence and lack of due diligence, one must ask, “What is the implication of not doing something” as well as of doing something?” Cyber security is no different, and as it relates to protection and control, can involve serious considerations with respect to the following areas:

- Legal
- Financial
- Safety
- Government Regulation
- Environmental

It is not the intention of this report to overreact to potential implications of a poorly designed security policy (or lack of a security policy) but to mention some issues that should be considered in giving cyber security due respect and attention.

Many people take for granted the safe and reliable operation of the power system and do not fully comprehend the amount of sophisticated equipment that is used in protecting the operation of the power system. With the proliferation of high-speed networks and the increased dependency on communications, there is serious potential for subversion on the reliable operation of the power system.

For example, in one case a disgruntled employee who was dismissed from his job was able to use a remote communication link to activate a SCADA system in a local waste water treatment plant and cause effluent to discharge in the neighbourhood. This network intrusion occurred numerous times before the culprit was apprehended. In another instance, hackers successfully infiltrated the computer system for the Salt River Project. The listing of examples can, unfortunately, be continued to some length. This list considers some of the possible ramifications arising from a cyber intrusion and is not intended to be exhaustive.

1.7 Security Threats and Vulnerability

1.7.1 Threats

In evaluating the security threat to substation equipment, it is apparent that numerous people have physical contact with various devices within the substation. These individuals include employees, contractors, vendors, manufacturers, etc. Of particular concern is the fact that the typical substation environment can provide a means to compromise the power system with a low probability being detected or apprehended. This low perceived probability of detection creates opportunities to compromise the operation of the power system which could be attractive for a number of reasons, including:

- Job dissatisfaction
- Economic gain
- Competitor discrediting
- Job security
- Blackmail
- Sport
- Terrorism/Political

The following list provides some examples of possible security threats that may exist in a substation (not to be considered all inclusive).

- A substation automation contractor, with access to the substation, recognizes the station has equipment from a competitor and seeks to discredit that competitor's system by modification of the system configuration.
- An employee concerned about future employment changes all passwords throughout the system so that only they can access the system.
- A third party provider/consumer of power with some authorization to the station arranges to have metering data improperly scaled to support compromised revenue meters.
- An authorized person is approached by a third party who offers financial reward for the point mapping, address, and password of the automation system.
- The vendor of the original system has left behind a backdoor which is unknown to the owner and can be used to change the configuration and performance of the system.

It is also important to consider the inadvertent compromise of an IED RET650 or automation system by authorized personnel who do not intend to degrade or affect its performance, but through some action on their part, do indeed compromise the device.

Examples include:

- The use of an out dated or incompatible configuration software version which results in a corruption of the substation device settings.
- The use/download of an incorrect configuration which results in incorrect settings.
- Errors in entering settings/configuration data or errors in the engineering development of settings/configuration which compromise the performance of the system.

The intentional and unintentional compromises of the power system are areas of concern for the NERC Cyber Security-Critical Cyber Assets and require addressing in any comprehensive cyber security program.

1.7.2 Threat Sources

In recent years, information security attack technology has become increasingly sophisticated. Attacks have become automated, so that specialized expertise is not necessarily required to perform them. Many attacks install “root kits” on the victim systems which are usually designed to enable the intruder to re-enter the system at will, to prevent the system administrator from discovering the attack, and to destroy any remaining evidence of the attack when the intruder is finished.

Threats may be caused by inadvertent actions of authorized persons as well as malicious actions of authorized and unauthorized persons. Some of the threat sources to consider include:

- Natural disasters and equipment failure
- Well-intentioned employees who make inadvertent errors, use poor judgment, or are inadequately trained
- Employees with criminal intent to profit or to damage others by the misappropriation of utility resources
- Disgruntled employees or ex-employees who cause damage to satisfy a grudge
- Hobbyist intruders who gain pleasure from unauthorized access to utility information systems (sport)
- Criminal activity by both individuals and organizations directed against the utility, its employees, customers, suppliers, or others
- Terrorists

- Competing organizations searching for proprietary information of the utility, its suppliers, or customers
- Unscrupulous participants in the markets for electric power or derivatives
- Software providers who, in attempting to protect their intellectual property rights, create vulnerabilities or threaten to disable the software in contractual disputes

In general, threats are directed towards information held by the utility, but the target of the threat may be an entity other than the utility, such as an employee, customer, or supplier. For example, reading residential electric use at frequent intervals can provide intruders information on when a residence is unoccupIED RET650. Also, the utility may store data on employees or customers that affects their privacy.

1.7.3 Vulnerabilities and Threats

- Device Level Threats and Vulnerabilities
  -

Chapter 2: Review of Internationally Accepted Standards and Guidelines (A Critical Evaluation)

As mentioned earlier in this project, cyber security for automation and control systems in the electric sector has gained considerable attention and importance over the last couple of years. While in the past, cyber security was not considered an issue or only “a nice-to-have”, it has become “a must-have”. In addition cyber security got special attention after several attacks were well covered in the media e.g. the Stuxnet attack. Several standards such as NERC-CIP, IEEE 1686 and IEC 62351 are addressing cyber security for control systems. Each of them covering and focusing on different areas and parts of the overall system leaving some gaps in between [14]. Fig 2.1 shows different standards and their application areas.

TC57 WG15 has started to address security for IEC TC57 communication protocols, particularly the IEC 60870-5, the IEC 60870-6 and the IEC 61850. Some parts of this technical specification have been finalized while work on other parts has just started. Performance evaluations of the official released IEC 62351 Part 6, performed by ABB, showed that both software as well as hardware implementations can today not satisfy the real-time requirements defined in IEC 61850 for GOOSE and SV data. TC57 WG15 has accepted these findings and is now looking at a new approach, in which authentication will be done using symmetric cryptography. TC57 WG15 is currently also starting to address certificate handling, which in the author views is the basis for all other IEC 62351 parts. These TC57 WG15 efforts, addressing cyber security issues, must be driven further so that security can become an integrated part of IEC 61850.

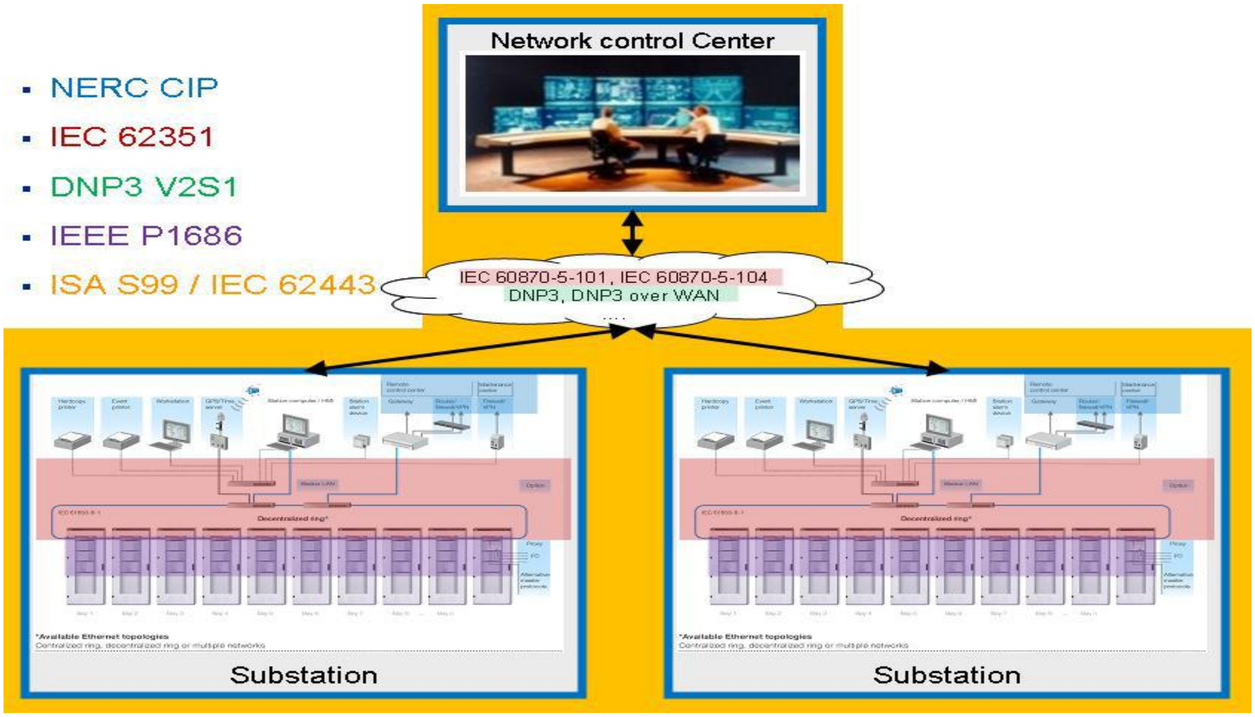
After all said, one should not forget that there are many other security mechanisms that can and must be used to improve the overall security architecture of modern substation automation systems. The fact that IEC61850 uses mainstream communication technology, i.e. Ethernet and TCP/IP, makes a wide variety of solutions available. Firewalls for examples can protect the security perimeter and VPN technology can build up secure channels to remote centers. Access to systems and devices have to be further protected by using user authentication and authorization coupled with detailed logging of all user activity.

As most substations and control centers are interconnected by a wide-area communication network, performance and security of such interconnections play a key-role in running the utilities core business in a highly reliable and efficient way. Even though the majority of these backbone networks are today SDH/PDH dominated, the usage of packet switched technology is increasing and along with it the security threats that need to be addressed carefully.

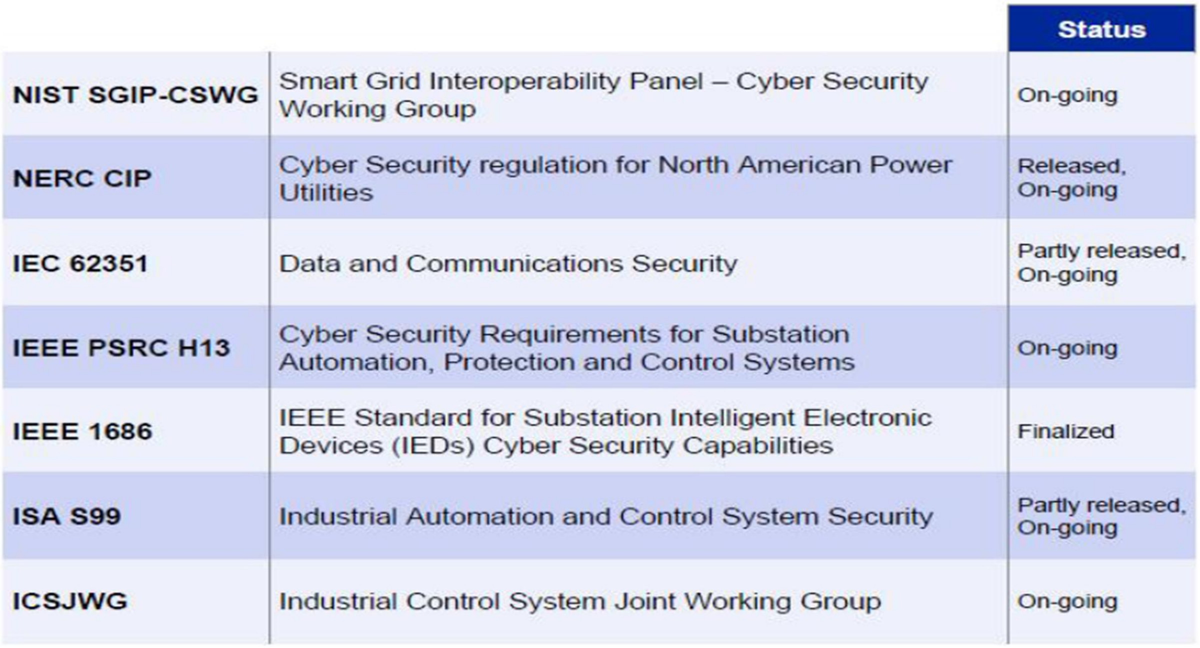
Substation automation, protection and control systems have changed significantly in the past decade. Systems have become more interconnected and provide end users with much more information to allow for higher reliability and increased levels of control. Interoperability between different vendor products and systems has been achieved by developing products and solutions based on open standards (e.g. IEC 61850 or IEC60870-5-104) and by leveraging hardened Ethernet technology.

This change in technology has brought huge benefits from an operational point of view, but it has also exposed utilities to similar cyber security threats that traditional enterprise systems have been confronted with since years. The fact that some utility applications have very stringent requirements for instance regarding timing (e.g. for IEC61850 GOOSE / SV messages), availability and environmental conditions (e.g. EMC) makes applying off the shelf technology for substation automation and communication equipment a challenging task and demands tailored solutions.

Several standards such as NERC-CIP, IEC 62351 and IEEE 1686 are addressing cyber security for control systems. Each of them covering and focusing on different areas and parts of the overall system leaving many gaps in between. The picture below shows those standards and their application areas.



The standards in this field are in different phases. Some have been finalized, some are still under development. For instance, the IEC 62351 standard, which secures all TC 57 protocols, is still under development. Some parts are being revised because the implementations based on the first versions have turned out to be difficult. The completed IEC 62351 Part 6 has been proven not to be feasible for practical implementation and a second edition is under way. Several important areas like Role Based Access Control or key handling have just been started and need some time until they are finalized. Following table 2 shows the status of several standards governing the field of cyber security for substation environment.



		Status
NIST SGIP-CSWG	Smart Grid Interoperability Panel – Cyber Security Working Group	On-going
NERC CIP	Cyber Security regulation for North American Power Utilities	Released, On-going
IEC 62351	Data and Communications Security	Partly released, On-going
IEEE PSRC H13	Cyber Security Requirements for Substation Automation, Protection and Control Systems	On-going
IEEE 1686	IEEE Standard for Substation Intelligent Electronic Devices (IEDs) Cyber Security Capabilities	Finalized
ISA S99	Industrial Automation and Control System Security	Partly released, On-going
ICSJWG	Industrial Control System Joint Working Group	On-going

Table 2. Status of Standards

It is clear from the above table that field of cyber security standards is far from over. Still lot of research work needs to be done and it will take lot of time and effort to mature these standards. Many critical questions are still un-answered which gives this area a huge potential for future research. None of the surveyed literature have anything concrete in terms of performance requirements thus there is still a question mark on Performance Requirements. Figure 2.2 shows two specific areas like GOOSE and Sampled Value processing which has entirely different performance requirements than what is required for client-server communication. Both these communications require real time priority communications which are not covered by normal client server arrangements [15].

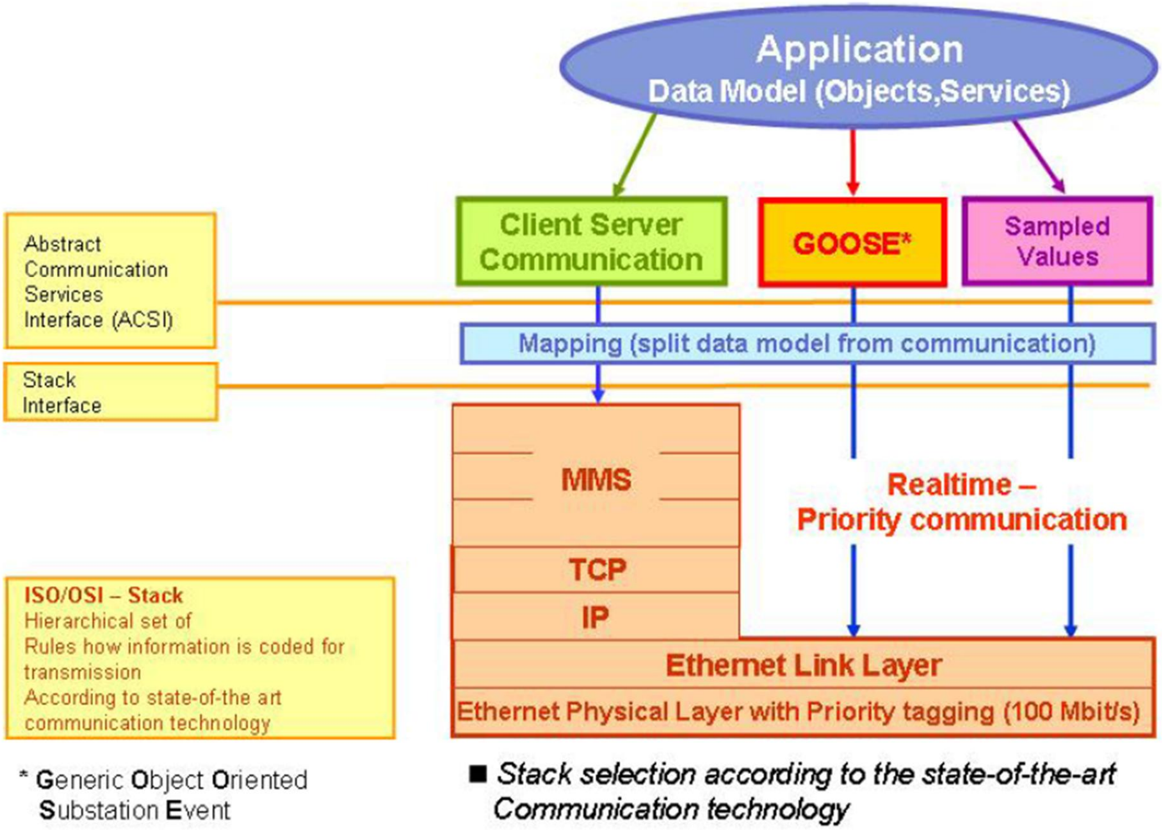
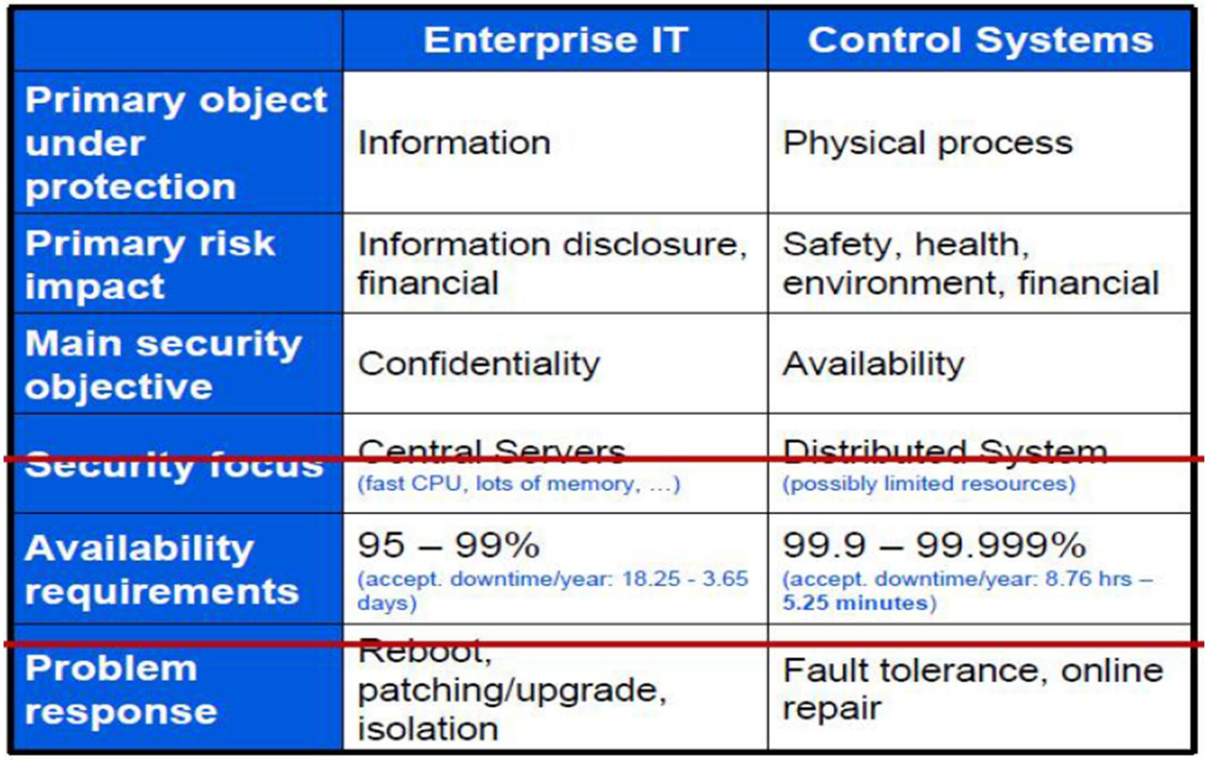

Application
Data Model (Objects,Services)
Abstract Communication Services Interface (ACSI)
Client Server Communication
GOOSE*
Sampled Values
Stack Interface
Mapping (split data model from communication)
MMS
TCP
IP
Realtime – Priority communication
ISO/OSI – Stack
Hierarchical set of Rules how information is coded for transmission
According to state-of-the art communication technology
Ethernet Link Layer
Ethernet Physical Layer with Priority tagging (100 Mbit/s)
* Generic Object Oriented Substation Event
■ Stack selection according to the state-of-the-art Communication technology

Fig 2.2. Stack Selection according to the Communication Technology

The most important thing to understand is the different requirements and entirely different set of goals for network security in IT Enterprise and Control Systems as shown in Table 3 below. Different parameters which differ in their importance and requirements for IT and Control Systems are:

- Primary object under Consideration
- Primary Risk Impact
- Main security objective
- Security Focus
- Availability requirements
- Problem Response

These parameters are described in the following table 3 as a function of their relation with IT Enterprise and Control Systems.



	Enterprise IT	Control Systems
Primary object under protection	Information	Physical process
Primary risk impact	Information disclosure, financial	Safety, health, environment, financial
Main security objective	Confidentiality	Availability
Security focus	Central Servers (fast CPU, lots of memory, …)	Distributed System (possibly limited resources)
Availability requirements	95 – 99% (accept. downtime/year: 18.25 - 3.65 days)	99.9 – 99.999% (accept. downtime/year: 8.76 hrs – 5.25 minutes)
Problem response	Reboot, patching/upgrade, isolation	Fault tolerance, online repair

Table 3. Difference Between IT and OT Networks

With the increased importance for cyber security of automation and control systems various working groups have taken on the topic in an attempt to provide standards, regulations, guidelines, or best practice documents. The focus, level of detail and maturity of these documents is quite broad and not all of them are equally applicable for substation automation, protection and control systems. At the moment five initiatives seem to be most advanced, which we will discuss in the following paragraphs.

NERC CIP

The NERC CIP regulations have had the biggest impact on electric utilities so far and been the focal point of most security programs. NERC CIP makes it very clear that the main responsibility for securing the electric grid lies with the utilities and that it is not just about technology. There are some shortcomings of the current version, i.e. the exclusion of serial protocols or the focus on a single electronic security perimeter, but these will likely be addressed in the currently ongoing 4th revision. The NERC CIP regulation is a good example of why compliance should not be the main goal of any security program. Because the regulation is changing and extending its scope utilities that focused their security program on complying to the versions currently in effect will run into problems with future releases.

NIST Smart Grid

Cyber security has been identifIED RET650 as a key enabler for the NIST Smart Grid activities and has gotten a lot of attention within the NIST driven Smart Grid activities. In February 2010 the second draft of the “Smart Grid Cyber Security Strategy and Requirements” document has been released for public comments. The document tries to take a holistic view of cyber security for Smart Grid, i.e. by looking at all applications of Smart Grid. The 2nd draft contains high level security requirements that will have an influence on substation automation, protection and control systems. However, at the time of writing it is not clear yet to what level of detail the requirements will be and how much tailoring needs to be done.

IEEE PES Substation C10 /PSRC H13

Within IEEE PES Substations and PSRC, a joint working group has been formed to look at the applicability and the technical implementation of the NERC CIP and NIST Smart Grid security efforts for substation automation, protection and control systems. The goal of the joint WG is to prepare a standard on “Cyber Security Requirements for Substation Automation, Protection and Control Systems” which provides technical requirements for substation cyber security. It presents sound engineering practices that can be applIED RET650 to achieve high levels of cyber security of automation, protection and control systems independent of voltage level or criticality of cyber assets. Cyber security includes trust and assurance of data in motion, data at rest and incident response.

IEC 62351

IEC 62351 is a technical security standard that aims to secure power system specific communication protocols such as IEC 61850 or IEC 60870-5-104. While most parts of the standard have been released in 2009 more work is needed before systems compliant to IEC 62351 can be put on the market. First of all the affected communication standards must be changed to support IEC 62351. In addition there are some technical challenges with securing real time traffic that must be addressed by the working group of IEC 62351.

IEC62351 has total of ten parts. Each part deals with a specific requirement in the field of substation control and automation as it comes to cyber security. Those parts are as follows:

1. Part 1: Introduction to Security Issues
2. Part 2: Glossary of Terms
3. Part 3: Profiles including TCP-IP
4. Part 4: Profiles including MMS
5. Part 5: Security for IEC60870-5 and derivaties
6. Part 6: Security for IEC61850
7. Part 7: NSM Data Object Model
8. Part 8: RBAC
9. Part 9: Key Management (not yet released)
10. Part 10: Security Architecture and Guidelines

IEEE 1686

Security of intelligent electronic devices is the scope of IEEE 1686. The document defines in technical detail security requirements for IED RET650's, e.g. for user authentication or security event logging. The standard very nicely points out that a) adherence to the standard does not ensure adequate cyber security, i.e. that adherence to the standard is only one piece in the overall puzzle, and that b) adherence to every clause in the standard may not be required for every cyber security program. With this the standard gives vendors clear technical requirements for product features but at the same time leaves room for specific, tailored system solutions at the customer site.

One could argue that why it is taking such a long time to finalize the standards around cyber security for substations. The idea and goals of TC57 WG15 to secure TC57 protocols look at a first glance logical and simple. But a deeper look into the challenges shows that it is not so trivial to achieve. Here are few reasons why it is taking so long and some of the major challenges to finalize the related to standards:

Real-Time constrains

Cryptography has to be used to secure today’s protocols. Unfortunately cryptography means mathematics and a lot of calculations which are time consuming. Many TC57 protocols are used in real-time applications in which reaction times cannot be longer than 1 or 2 milliseconds. Unfortunately the more secure the protocols become, the slower the reaction times will be.

Methods lifetime

Security methods and algorithms have to be updated regularly, methods and algorithms picked a few years ago are today broken, as an example we have the hash algorithms case: MD5 was replaced with SHA-1 and now SHA-1 is being replaced by SHA-256, which itself will have to be replaced a few years from now. So by the time a security standard reaches the maturity to be released, its algorithms and methods will probably be obsolete or unsecure.

Consensus

As with all standards, common consensus has to be reached among all members working and reviewing the standards (vendors, countries, etc.). There are a lot of players with different security cultures and it takes time for all to agree on all issues. So agreement in all details of a standard takes long.

Still even when we overcome all these hurdles listed above and the standards are signed off, there will be the need for huge investments to replace existing devices (so the devices can handle cryptography and they provide minimal security features, such as secured non-volatile memory to store device cryptography keys).

Some of the excerpts of these two most important standards (IEC62351 and IEEE1686) are provided in APPENDIX A at the end of project documentation for reference purposes.

Chapter 3: Brief Overview of Cyber Security related Theoretical Concepts

Generally speaking, here are various forms of access control and other cyber security functions related to substation automation and control.

3.1 Role-Based Access Control (RBAC)

Role Based Access Control essentially implements the separation of duty approach that has long been taken by businesses in protecting the integrity of their business processes and critical data. Interest in RBAC arose as a result of an evaluation of information security technology, which at one time was focused on the confidentiality needs associated with military and diplomatic matters. Recognition that business (and some government) applications are more focused on the need for integrity resulted both in the development of the Common Criteria for Information Security Evaluation (ISO 15408) and research attention to RBAC. Indeed, one of the first examples of a Protection Profile prepared and published using the Common Criteria was a specification for evaluating RBAC.

The description of RBAC presented here is based on a proposed standard for RBAC prepared by NIST (available at http://csrc.nist.gov/rbac/) [12]. Under the proposed standard, RBAC deals with the elements of Users, Roles, Objects, Operations, and Permissions. A user is a person, but can be extended to a process. A role is a job function within the context of an organization. A user may be assigned multiple roles and a role may be occupied by multiple users, although the relationship between users and roles may be limited by constraints. Objects and operations depend on the system context. For example, in a DBMS an object may be a table and an operation may be a select or update. A permission is the approval to perform the operation on the object.

Core RBAC requires the capabilities to manage assignment of users to roles and manage assignment of permissions to roles. It requires that a user be able to assume multiple simultaneous roles. The proposed standard describes this as capturing the functionality of group permissions in current operating systems.

Hierarchical RBAC introduces role hierarchies, with senior roles in the hierarchy inheriting the permissions of their juniors and users assigned to senior roles being assigned as well to the associated junior roles. Constrained RBAC introduces separation of duty relationships, which are static or dynamic constraints on the roles to which a user can be simultaneously assigned. An example of a static constraint is that a billing clerk is never allowed to also be an accounts receivable clerk. An example of a dynamic relationship is that the originator of a document is never also allowed to be the approver of the same document, but may approve other documents.

3.2 Discretionary Access Control (DAC)

Discretionary Access Control is the traditional “user group- other/read-write-execute” type of control traditionally found in operating systems and DBMS’s. It is also the kind of control provided by access control lists. Under DAC, the owner of the data or file essentially has discretion to provide access to whoever the owner determines should have access. The system enforces the owner’s access decision, but does not otherwise enforce constraints on access to the data. DAC is one means of enforcing Need-to-Know, where it is assumed that the security structure and policies are such that the “owner” of data knows who has need-to-know.

3.3 Mandatory Access Control (MAC)

In the traditional definition of Mandatory Access Control, objects (e.g., data) and subjects (e.g., users, devices) are given sensitivity labels according to a hierarchy. The label is part of the access control associated with the subject or object. Security policies govern the access and movement of objects by subjects. The most well-known MAC security policy is the “Bell LaPadula Security Model” that prohibits a subject having a lower level sensitivity label from reading an object having a higher sensitivity label and also prohibits a subject having a higher level sensitivity label from writing an object to a subject (e.g., a user directory or a printer) having a lower sensitivity label. The policy is often summarized as “No read up, no write down” and is enforced by the operating system.

3.4 Authentication

Authentication is the process of determining that the user is authentic, i.e., that the user is who the user claims to be. This is done by receiving information about the user and comparing the received information to a stored version of the information for the authentic user. Up to three factors may be used:

- Something the user knows, such as a password
- Something the user has, such as a device or smartcard, usually identifIED RET650 by some kind of encrypted information. Some devices automatically change the information periodically in synchronism with other software or devices in the authentication system.
- Something the user is, essentially data regarding a biometric characteristic of the user, such as a fingerprint or eyeball pattern, generally stored in some encryption protected format.

There are numerous ways in which an authentication system can be attacked and compromised. These include various means of tricking a user into revealing a password, various strategies for guessing passwords and validating the accuracy of the guesses, and various methods of capturing passwords (or other authentication information) as it moves in the system. There are also ways in which an authentication system can be bypassed, essentially involving attacks on the security of the overall system.

3.5 Captured User Approaches

A captured user approach involves “capturing” or “jailing” the user to prevent any access to capabilities that a malicious user could exploit to engage in unauthorized activities on the system. For example, this would generally involve sending the user from system login directly into a menu system from which the user can't escape. Sending the user into the menu system generally involves a function that is automatically executed upon startup of a computer or upon user login. However, there are a wide variety of system functions that must be blocked to ensure that the user remains captured.

In general, the capturing fails if a user is able to access a system prompt, or also in the case of interpreted languages an interpreter prompt, that enables access to commands that can be used for performing functions that support disallowed activity. Among other things, this may mean that the user must be prevented from starting the system or logging in without going through the auto-execute function that starts the menu system. It means that functions that can stop a process and return to the system prompt (such as Control-C or Control-Z on some systems) must be disabled. It means that any exception that could result in a crash leading to a language interpreter prompt must be handled and returned instead to the menu system. It is best if functionality not needed by a legitimate user is not present on the system.

Captured user approaches are good for purposes such as specialized kiosk-type terminals having well-defined, limited uses. Also, any user accessing a web page is essentially a captured user of the system containing the web server.

3.6 Encryption

Encryption is another important security protection used in both stand-alone systems and networks. Encryption modifies a file or message so it cannot be read without reversing the modifications using another piece of information called an encryption key (often shortened to key). The modifications usually involve substituting characters for those in the message or transposing (rearranging) the locations of either the original message characters or the substituted characters. The key provides data needed for controlling the substitutions and transpositions. The calculations are performed according to an encryption algorithm. Sometimes, for user convenience, the encryption key is generated from a password as part of the algorithm.

Encryption technology can be used for a variety of purposes. Examples include encryption of messages sent over communication lines, encryption of passwords stored on a computer, exchange of encryption-based information to authenticate user identity, creation of encryption-based checksums (called hashes) to verify the integrity of transmitted data, and use of encryption technology to digitally sign documents. There are a variety of methods for digital signature, all relying on encryption for verifying that a document originated from a particular source. Most of these methods use public key concepts that are discussed in the next section.

3.7 Key management and public key cryptography

Management of the encryption keys is a major issue in managing an encryption system, and tends to drive the technology of encryption systems. It is also a major source of vulnerability exploited in code-breaking.

The most convenient system is one in which the key is automatically generated from a short password used over and over again. The password can be the same for all users or different for different groups of users. However, this system is also less secure. The more often the password is used, the greater is the opportunity for compromise. There are also the issues of choosing the passwords themselves, deciding how often they should be changed, and securely providing this information to all the users.

A common practice in key management is to use a hierarchy of keys having various lifetimes. The higher level keys in the hierarchy are used only for the purpose of exchanging lower level keys. The lowest level key in the hierarchy is called the session key and is used only for encrypting a limited number of messages.

Another problem in key management occurs when the sender and recipient have not been able to prearrange a key or password. This situation can be expected to occur often in electronic commerce. One solution is to use a trusted third party with whom both sender and receiver have already prearranged keys. Another solution is known as public key cryptography. This solution uses a pair of related mathematical functions, one of which is easy to calculate and the other of which is very difficult. One pair of such functions is multiplication and factoring. It is easy to multiply large numbers but very difficult to factor a large number into its prime components.

The approach offered by these solutions is to provide two keys, one a public key that is published and made available to potential senders and the other a private key that is kept secret by the owner. A message encrypted using the public key can be decrypted only with the private key and vice versa.

Public key cryptography is often used as a means of facilitating key management and as an adjunct to other systems of encryption. For this purpose, the public key cryptography is used for exchanging session keys in the other encryption system. Public key cryptography is also used as a means of digital signature. A signature encrypted with a user's private key can be verify using the associated public key.

The most secure encryption method -- called the one-time pad – was developed in 1917 for use in World War I and uses a key that is completely random and is as long as the message to be sent. Only two physical copies of the key exist, one for the message sender and the other for the message recipient. The key is used once and then destroyed. The problem with this type of system is that enough key material to handle all messages has to be prepared and securely distributed to every sender and every recipient. The material has to be securely stored and destroyed after use. If a sender and recipient run out of key material, they cannot send and receive messages until fresh key material arrives at both locations. This system is very secure -- theoretically unbreakable if the key is derived from a random physical process -- but very inconvenient. However the system becomes subject to code breaking if the key material is used more than once, e.g., if a message must be sent and there is no fresh key material available.

In a layered communications protocol system there is a trade off in the placement of the encryption in the protocol stack. Placement near the application layer allows the encryption to be tailored to the importance of the data and ensures that only the application itself actually sees the unencrypted data.

However, this placement also exposes information about message flows such as date, time, addressee, message length, and (if the protocol system has a capability for priority transmission) other information such as the urgency of the message. Placement close to the physical layer can conceal message flow information but also exposes the information within the node outside the using application. Placement in both locations provides better protection but creates a more complex system.

Even with successful encryption an eavesdropper can still obtain information by watching a data stream. The technique for doing so is called “traffic analysis” and was also developed during World War I. It involves watching the patterns of message activity and correlating these patterns with the observable operational situation. When a pattern repeats, it can be inferred that the corresponding operational situation is occurring. Defeating traffic analysis requires that communications channel activity be modified to avoid patterns, such as by keeping channels active with dummy traffic in the absence of actual message traffic, or by taking other steps to avoid allowing patterns to be correlated with operational conditions.

Chapter 4: Suggested Approach to Cyber Security

The most important principle for any security architecture is defense-in-depth as shown in Figure 4.1. Having a single layer of defense is rarely enough as any security mechanism may be overcome by an attacker, It is therefore recommended to architect the system in a way that the most sensitive parts of the system are protected by multiple rings of defense that all have to be breached by the attacker to get to those “crown jewels”.

In addition not only protection mechanisms should be deployed but also means of detecting attacks. This includes both technical measures, such as intrusion detection systems, as well as procedural measures, such as review of log files or access rights.

When we look at the organizations involved in maintaining utility system security—vendors, integrators, end users—it’s fair to say that security is “everybody’s business.” To the extent these groups cooperate with one another throughout the system lifecycle, security will be enhanced. At the same time, perhaps the most important aspect of security for the various players to keep in mind is that it is a journey and not a destination. There will always be new threats. Likewise, there will be new methods and technologies for meeting those threats. Vigilance, cooperation and technical expertise, when applied in union, offer the best defense.

4.1 Defense in depth

Power system operations pose many security challenges that are different from most other industries. For instance, most security measures were developed to counter hackers on the Internet. The Internet environment is vastly different from the power system operations environment. Therefore, in the security industry there is typically a lack of understanding of the security requirements and the potential impact of security measures on the communication requirements of power system operations. In particular, the security services and technologies have been developed primarily for industries that do not have many of the strict performance and reliability requirements that are needed by power system operations. Figure 4.1 shows an overall view of defense in depth as applied to a substation automation system. It includes the following:

- Client Server Authentication
  - Exchange of X.509 Standard certificates

- Recommended Cipher suite
  - Key Exchange via RSA
  - Data Encryption via AES 128 bit
  - Recommended Hash function SHA-1 (160 bit)
  - Message digest MD5 algorithm

- System Hardening for Servers and Workstations.
  - Removal of unused software
  - Disabling the unused services
  - Removal of unused accounts
  - Change of default passwords

- Access Control and Least privileges Principle
  - Role Based Access Control (RBAC) to limit access privileges
  - Password restrictions
  - Possibility to have personal accounts

- Network System Hardening
  - Disabling the unused services
  - Removal of unused accounts
  - Change of default passwords

- Network Separation
  - Avoid flat networks. Use firewalls, gateways, etc to create network zones.
  - Create DMZ (demilitarize zone) for all external access
  - Filter both incoming and outgoing traffic between zones
  - Use VPN connection outside a firewall

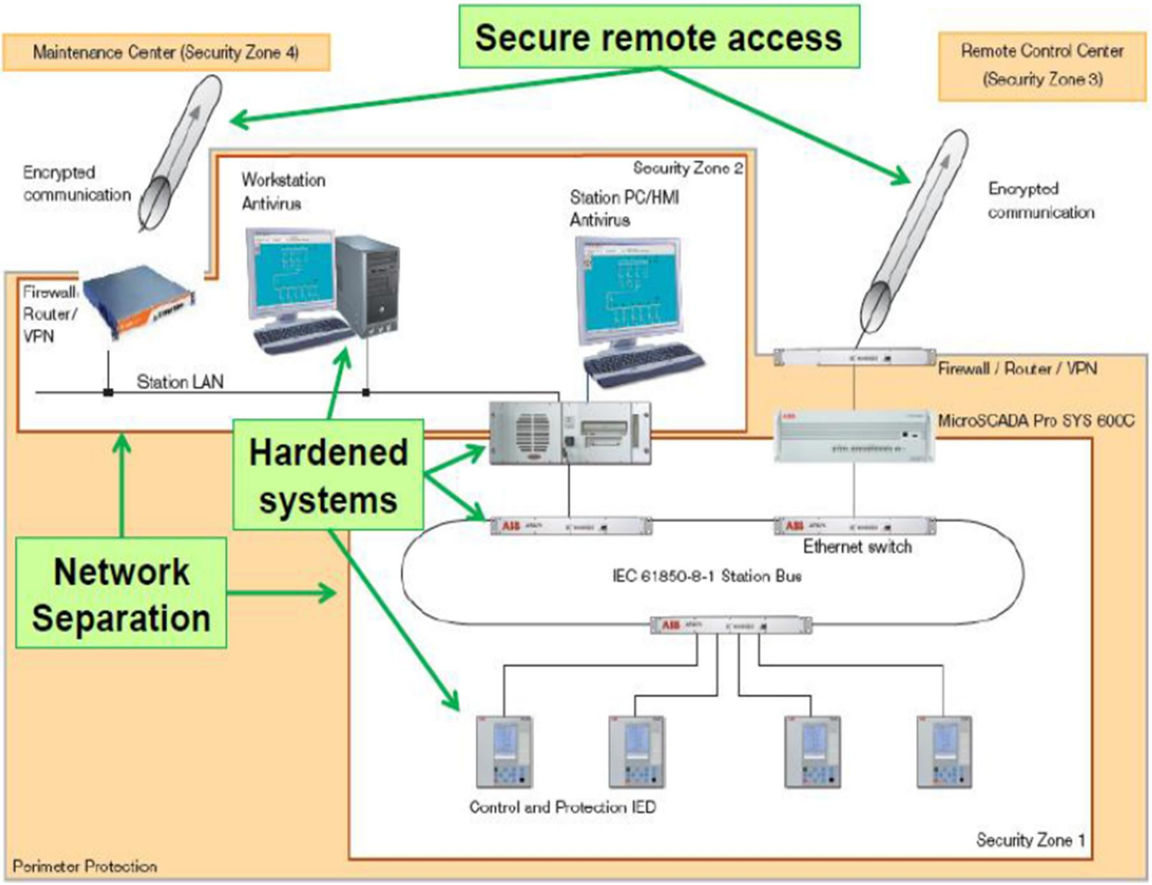


Fig. 4.1 Defense in Depth

4.2 LAN / IP Security

Because of the large variety of communication methods and performance characteristics, as well as because no single security measure can counter all types of threats, it is expected that multiple layers of security measures will be implemented. For instance, VPNs only secure the transport level protocols, but do not secure the application level protocols, so that additional security measures, such as IEC 62351-4, provide the application level security, possibly running over VPNs. In addition, role-based access passwords, intrusion detection, access control lists, locked doors, and other security measures are necessary to provide additional levels of security. It is clear that authentication plays a large role in many security measures. In fact, for most power system operations, authentication of control actions is far more important that “hiding” the data through encryption.

As connection to the Internet is (should not be) a factor, since power system operations should be well-protected by isolation and/or firewalls, some of the common threats are less critical, while others are more critical. Although importance of specific threats can vary greatly depending upon the assets being secured, some of the more critical threats are:

- Indiscretions by personnel – employees stick their passwords on their computer monitors or leave doors unlocked.
- Bypass controls – employees turn off security measures, do not change default passwords, or everyone uses the same password to access all substation equipment. Or a software application is assumed to be in a secure environment, so does not authenticate its actions.
- Authorization violation – someone undertakes actions for which they are not authorized, sometimes because of careless enforcement of authorization rules, or due to masquerade, theft, or other illegal means.
- Man-in-the-middle – a gateway, data server, communications channel, or other non-end equipment is compromised, so the data which is supposed to flow through this middle equipment is read or modifIED RET650 before it is sent on its way.
- Resource exhaustion – equipment is inadvertently (or deliberately) overloaded and cannot therefore perform its functions. Or a certificate expires and prevents access to equipment. This denial of service can seriously impact a power system operator trying to control the power system.

4.3 Procedural Security

1) Communications Network Management: Monitoring the Networks and Protocols:

- Detecting network equipment permanent failures
- Detecting network equipment temporary failures and/or resets
- Detecting network equipment failovers to backup equipment or communication paths
- Detecting the status of backup or spare equipment
- Detecting communication protocol version and status

- Detecting mis-matches of differing protocol versions and capabilities
- Detecting tampered/malformed protocol messages
- Detecting inadequately synchronized time clocks across networks
- Detecting resource exhaustion forms of Denial of Service(DOS) attacks
- Detecting buffer overflow DOS attacks
- Detecting physical access disruption
- Detecting invalid network access
- Detecting invalid application object access/operation
- Ability to detect coordinated attacks across multiple systems
- Collecting statistical information from network equipment; determining average message delivery times, slowest, fastest, etc. and counting number of messages, size of messages
- Providing audit logs and records

2) Communications Network Management: Controlling the Networks:

- Manual issuing of on/off commands to network equipment
- Manual issuing of switching commands to network equipment
- Setting parameters and sequences for automated network actions
- Automated actions in response to events, such as reconfiguration of the communications network upon equipment failure

3) System Management: Monitoring Intelligent Electronic Devices (IED RET650s)

- Numbers and times of all stops and starts of systems, controllers, and applications
- Status of each application and/or software module: stopped, suspended, running, not responding, inadequate or inconsistent input, errors in outputs, error state, etc.
- Status of all network connections to an IED RET650, including numbers and times of temporary and permanent failures
- Status of any “keep-alive” heartbeats, including any missed heartbeats
- Status of backup or failover mechanisms, such as numbers and times these mechanisms were unavailable

- Status of data reporting: normal, not able to keep up with requests, missing data, etc.
- Status of access: numbers, times, and types of unauthorized attempts to access data or issue controls
- Anomalies in data access (e.g. individual request when normally reported periodically)

4) System Management: Control Actions within Intelligent Electronic Devices (IED RET650s):

- Start or stop reporting
- Restart IED RET650
- Kill and/or restart application
- Re-establish connection to another IED RET650
- Shut down another IED RET650
- Provide event log of information events
- Change password
- Change backup or failover options
- Providing audit logs and records

4.4 Password and Key Management

The following discussions are an extract from FIPS PUB 112, Appendix A.

1) Password Usage

a) Introduction

This appendix contains background information, a discussion of the factors specify IED in the Password Usage Standard and the rationale for the minimum criteria specify IED in the Standard. It also provides guidance in selecting parameters of password systems based on increasing security requirements. Examples of three password systems meeting increasing levels of security requirements are included.

b) Background

Passwords are the most common method of personal identification used in conjunction with remote terminals to deter unauthorized access to computer systems and networks. The effectiveness of passwords has often been questioned, primarily because they can be easily forgotten or given to another person. However, passwords can provide reasonable deterrence to unauthorized access if properly handled by people authorized to use them and if properly stored and processed in the password verification system. Within its Computer Security and Risk Management Program, the Institute for Computer Sciences and Technology of the National Bureau of Standards developed this Standard for secure password usage to assure reasonable handling, storage and processing of passwords.

Shortly after issuing FIPS PUB 48, NIST published Special Publication 500-9, The Use of Passwords for Controlled Access to Computer Resources. This publication considered the generation of passwords and their effective application to the problem of controlling access to computer resources. Following analysis and use of this document, a project was initiated to establish a fundamental performance standard for the use of passwords and a guideline on how to use this Standard to achieve the degree of protection that passwords were intended to provide.

The Password Usage Standard was developed within the Computer Security and Risk Management Program of the Institute for Computer Sciences and Technology with considerable assistance from representatives of Federal organizations and private industry. In 1980, NIST developed and distributed a draft Password Usage Standard to

government and industry representatives for comments and then held a workshop to discuss the benefits and impact of the draft Standard. The draft Standard identify IED 10 factors to be considered in the implementation of password systems and quantify IED security criteria in a hierarchical manner for each of the 10 factors. It also proposed five levels of security and specify IED minimum criteria for each level. The workshop participants felt that the 10 factors were useful in structuring the design of password systems, but that the proposed five levels were unworkable as a basis of a password Standard. As a result of the workshop recommendations, the Standard was revised to specify minimum criteria for the factors of a password system. An Appendix was drafted which provided guidelines for achieving higher levels of security. This revised Standard and the draft guidelines were published for public comment and for agency comment in July, 1981. The received comments were used in revising the proposed Standard and draft guidelines in preparing the published Standard and guidelines.

c) Factors

Ten factors of an automated password system are specify IED in the Standard. These factors constitute the fundamental elements which must be considered, specified IED and controlled when designing and operating a password system. The rationale for the factors and for the minimum acceptable criteria for the factors specified IED in the Standard are provided in the following discussion. Guidance on how to meet the minimum criteria and reasons for exceeding the minimum criteria are also provided.

d) Composition

A password is a sequence of characters obtained by a selection or generation process from a set of acceptable passwords. A good password system has a very large set of acceptable passwords in order to prevent an unauthorized person (or intruder) from determining a valid password in some way other than learning it from an authorized person (i.e., owner). The set of acceptable passwords should be large enough to assure protection against searching and testing threats to the password system (and hence the data or resources that it protects) commensurate with the value of the data or resources that are being protected. The set of acceptable passwords must be such that it can be specified IED easily, that acceptable passwords can be generated or selected easily, that a valid password can be remembered, can be stored reasonably, and can be entered easily. Composition is defined as the set of characters which may comprise a valid password.

The composition of a password depends in part on the device from which the password is going to be entered. It also depends on how and where the password is going to be stored and how the stored password will be compared with the entered password. Federal Information Processing Standards Publication 1-2 (FIPS PUB 1-2) incorporates the American Standard Code for Information Interchange (ASCII) which specifies a set of characters for interchanging information between computers. Federal Information Processing Standards Publication 1-2 (FIPS PUB 1-2) defines several proper subsets of this set to be used for special applications. The 95-character graphics subset specified IED in FIPS PUB 1-2 is the set from which the System Manager and Security Officer should select the acceptable composition for a particular system. While backspaces can be used effectively to mask printed passwords, several comments on the draft guidelines described the special use of backspace in many computer systems and recommended that it not be allowed.

The minimum composition contains 10 characters because some systems (e.g., financial transaction systems) use a 10-digit PIN PAD (Personal Identification Number entry device) for entering the password which is called a PIN. The PIN PAD looks very similar to the keyboard of a push button telephone. Some systems being developed use the push button telephone for data entry and retrieval. Users of these systems stated their desire to use the Standard. A better composition contains 16 characters which includes the 10 digits plus (A, B, C, D, E, F). This set can represent hexadecimal characters, each of which is a four-bit (binary digit) code. For example, 16 hexadecimal characters are used to represent a Data Encryption Standard key (see FIPS PUB 46) which can be used as a personal key in a cryptographic system. Many passwords are composed only of the 26 lower case letters (a-z) or the 26 upper case letters (A-Z). However, using either of these sets often encourages the selection of a person's initials, name, nickname, relative, hometown, or common word easily associated with the person. Even allowing all possible 4-letter, 5-letter or 6-letter English words greatly restricts the number of passwords when compared to all possible passwords of length range 4-6 with the same composition. Totally alphabetic password composition should be discouraged. The best password composition is the 95- character graphic set as specified IED in FIPS PUB 1-2.

e) Length

Length is closely associated with composition in assessing the potential security of a password system against an intruder willing to try exhaustively all possible passwords. The length of a password provides bounds on the potential security of a system. A length of exactly 1 reduces the potential number of valid passwords to the number of characters in the acceptable composition set. A length of 2 squares this number; a length of 3 cubes this number; a composition of 10 and a length of exactly 4 provides for 10- (read 10 raised to the fourth power) or 10,000 possible passwords. PINs are typically four digits because of low security requirements, for ease of remembering by a large customer base and for speed and accuracy of entry. A PIN verification system generally prevents a person from quickly trying all 10,000 possible PIN's for a particular valid financial account in order to find the valid PIN. If the trial and error process can be automated, even on a small home computer, the valid PIN can be found in a few minutes. Having a length range of 4-6 increases the possible number of PIN's to 1,110,000 (106+105+104).

If all other factors are temporarily ignored, the security provided by a password is directly proportional to the allowed length of the password. In other words, longer passwords are more secure. However, other factors cannot be ignored in practical password systems. Long passwords take longer to enter, have more chance of error when being entered, and are generally more difficult to remember (the latter may not be true unless the password consists of random characters). Sixteen random hexadecimal characters are very difficult to remember and are very difficult to enter quickly and accurately. For this reason, DES keys are usually not personal passwords and vice versa. However, long passphrases can be transformed to virtual passwords of exactly 64 bits (or 56 bits with the other 8 bits recomputed to be parity bits). Long passphrases can be easy to remember but still take longer to enter.

The length range should include a number of lengths, probably from 5-8 characters, and the composition should be a large set so that a high level of security can be provided easily.

A passphrase is an understandable sequence of words (sentence, sentence segment, phrase) that can be transformed and stored as 64 bits, and which is used as a password. A passphrase is generally easy to remember by the owner of the passphrase, and hence is allowed on some systems because of this characteristic. Since the number of distinct possibilities of understandable passphrases is considerably smaller than for a random sequence of characters of the same length, a longer passphrase is preferable to a shorter one. For example, the number of understandable 64-character long passphrases composed using the 27-character set A-Z and space, is considerably less than 2764, which is the number of possibilities if the characters are selected randomly.

A passphrase may be used that is equivalent to a password as specified IED in the Standard. A passphrase may be transformed into a virtual password by using a transformation such as a hashing function or a cryptographic function. These functions should compute a value using the entire passphrase as input such that any change in the passphrase should result in a different computed value (within some probability). The value that is computed is the virtual password and must be 64 bits as specified IED in the Standard. This allows all password systems to allocate a maximum of 64 bits for storing each password, and therefore allows up to 264 possible passwords (many thousands of years of security against exhaustive searching attacks). Such a passphrase thus provides the benefits of being easily remembered at the added cost of additional time to enter the longer passphrase and the time needed to compute the virtual password.

f) Lifetime

The security provided by a password depends on its composition, its length, and its protection from disclosure and substitution. The risk associated with an undetected compromise of a password can be minimized by frequent change. If a password has been compromised in some way and if a new password is created that is totally independent of the old password, then the continued risk associated with the old password is reduced to zero. Passwords thus should be changed on a periodic basis and must be changed whenever their compromise is suspected or confirmed.

The useful lifetime of a password depends on several variables, including:

- The cost of replacing a password
- The risk associated with compromise
- The risk associated with distribution
- The probability of "guessing" a password
- The number of times the password has been used
- The work of finding a password using exhaustive trial and error methods

Password systems should have the capability of replacing the password quickly, initiated either by the user or the Security Officer. Passwords should be changed voluntarily by the owner whenever compromise is suspected and should be changed periodically with a maximum interval selected by the Security Officer. The interval may be a period of time or depend on a number of uses. The password system itself should have automated features which enforce the change schedule and all the security criteria for the installation. The system should check that the new password is not the same as the previous password. Very sensitive applications may require that a new password not be the same as any of the previous two, three, ..., N passwords. Such a system requires storage for N passwords for each user. It should not be a requirement of a system that the password for each user be unique. Having a new password rejected for this reason confirms that another user has the password.

g) Source

Passwords should be selected at random from the acceptable set of passwords by either the owner or the password generator. However, this guidance may not be possible in all cases and may not be desirable in some cases. The Security Officer often selects a password for a new user of a system. This can be used for the first access to the system. The system may then require that the user replace this password which the Security Officer may know with a password that only the user knows. Passwords that are created or selected by a user should be checked by the automated password system as meeting all of the criteria of the password system. Passwords that do not meet all the criteria should be rejected by the automated password system. A record that an attempt to select an unacceptable password may be made by some automated systems but is not required by the Standard.

If passwords are generated by the system, the method of generation should not be predictable. Commonly used random number generators that are available in computer systems for statistical purposes should be avoided because the sequence of random numbers that they generate are predictable. The DES algorithm, together with a nondeterministic parameter such as the least significant bits of a high resolution computer system clock may be used. The results of a random generator are then combined with password selection rules to obtain a password which meets mandatory and desirable criteria.

h) Ownership

A personal password should be individually owned rather than owned in common by a group of individuals in order to provide individual accountability within a computer system. This is desirable even though a group of people all have common access privileges to the same resources or data. Individual ownership of personal passwords is required because:

- It can establish individual accountability for the determination of who accessed what resources and for what purposes
- It can establish illicit use of a password or loss of a password
- It can be used for an audit trail of the activities of a user
- It avoids the need to change the password of an entire group when a single member of the group leaves or loses authorization privileges

i) Distribution

A password must be transported from the owner to the authentication system if selected by a user, from the authentication system to the owner if generated by the password system or from the Security Officer to both the owner and the authentication system if generated by the Security Officer. The initial password is often distributed in a different manner than subsequent replacement passwords. The initial password is generally created and issued directly, either orally or in writing, during the meeting at which a user is initially authorized use of the computer system or access to a set of data. This may be a one- time password which must be changed after the initial access request is granted. Changing of a password by a user generally requires that the user supply the old password and then the replacement password. The replacement is checked for meeting the security requirements of the system, checked that it is different than the old password, and then entered into the storage location of the old password. An audit record should be made of the replacement, containing the date and time of the change, but not the new password. Forgotten passwords should be replaced and a new password issued in a manner similar to, if not identical with, issuance of the initial password.

Passwords that are distributed in writing should be contained in a sealed envelope marked "To be opened by addressee only." Delivery may be by courier, internal 'mail, or by U.S. Mail. Instructions to the user should be to:

- Destroy the written password after memorizing it; or

- Return the written password to the Security Officer after signing the receipt for the password and after sealing it in the return mailer.
- Use the password as soon as possible and, if the password can be changed by the user, change the password.

Some systems distribute passwords in a sealed mailer that has been printed by a computer. The mailer is designed so that it cannot be resealed once it is open. The password is printed only on the inside of the mailer on the second page using carbon paper attached to the back of the mailer's front page. The instructions say to remove the front of the mailer, which shows the name of, 'the intended recipient, to destroy the front and save the password (in a protected place readily accessible only to the intended recipient). The part of the mailer that has the password has no other identification which would associate the password with either the system or the owner. Thus, anyone finding a lost password would usually not be able to use it. While not as desirable as memorizing the password and destroying the distribution medium, this system is useful when passwords are not routinely used and would be written in a location which-is more easily associated with the owner.

When distributed by a secure mailer, a receipt for the password may be validated by positive response or on an exception basis. When password distribution is done on an unscheduled basis, a positive response is required. When passwords are distributed regularly, the user should be expecting a new password and should report any failure to
obtain a new password. In either case, a record must be kept of the fact that a new password was issued.

There may be a transition period in which it is uncertain if the old password is valid or if the new password is valid. Some systems may allow either password to be valid during the transition period. This means that both passwords must be stored and compared with an entered password. Some systems may have no transition period (e.g., a password becomes valid at 8:06 P.M. exactly) and record attempts at using the old password in an audit file. A report of such attempts should be sent securely to the password owner as notification that usage of an old password was attempted. The owner can verify that the use was an accidental rather than an unauthorized use of an old password by an intruder.

j) Storage

Passwords should be stored in the authentication system in a manner which minimizes their exposure to disclosure or unauthorized replacement. Several methods have been used to protect passwords in storage. Most systems have a password file that can be legitimately read only by the "LOGON" program. The file is protected by a file access mechanism which checks a protection bit in a file access table. Only the privileged LOGON program has access to read the file and only the password program has access to write the file. Some systems separate the password file from the authorized user file. An index file is used to provide the correspondence between the user and the user's password. Some systems encrypt the passwords, either reversibly (two way) or irreversibly (one-way) using a Data Encrypting Key (DEK) or the password itself as a key. Of course, any key (e.g., a Data Encrypting Key) retained in storage would also need protection by encryption using a Key Encrypting Key (KEK). The type of protection provided to the passwords should be commensurate with the protection desired for the system or data and hence a protection system should be used to provide the desired protection.

One-way encryption of passwords is allowed in the Standard when encryption is used for stored password protection. One-way encryption systems transform the password in such a way that the original password cannot be recovered. This protects the original password from everyone, including the Security Officer and the systems programmers. When a user is logging onto such a system, the password that is entered by the user is one-way encrypted and compared in encrypted form with the stored encrypted password. The same encryption method and key must be used to encrypt the valid password before storage and to encrypt the entered password before comparison.

Two-way encryption of passwords is also allowed in the Standard. Given the correct key, the original password may be determined from the encrypted password. A user entered password may be compared with the decrypted stored password (which was encrypted), or the user's password may be encrypted and compared with the stored password as is done with one way encrypted passwords.

k) Entry

Entry of a password into an automated authentication system in a secure manner is often a difficult task. An observer often is able to detect part or all of a password while the user is entering the password. Typing keyboards are the typical entry device. A user that is not a trained typist often enters the password with one finger. A long, random password that is difficult to enter may be more vulnerable to observation than a short easily entered password. The Standard specifies that a password shall be entered by a user in such a manner that the password will not be revealed to anyone observing the entry process. The following discussion provides some techniques which the user may find useful in achieving this goal and which the computer systems operation staff may find useful in assisting the user.

The computer terminal, keyboard, push-buttons, or password entry device should provide a means for minimizing the exposure of the password during entry. The password should not be printed on the terminal during the entry process. If the keyboard and the terminal display or printer are directly coupled, then the password should be masked by obliterating (under striking) the space where the password is going to be printed. The password may be masked further by overstriking the area after password entry. Computer generated masks used during password entry to disguise the entered password should not always be the same. In any case no printed or displayed copy of the password should exist after password entry.

CRT terminals which use half-duplex communications may present a problem because the password overwrites the Under striking and remains visible on the display. The display should be immediately cleared by the password entry program after password entry in such systems. Users should be instructed to manually clear the display following password entry if the screen cannot be cleared by the password entry program.

When submitted as a part of a remote entry batch processing request, the password should be added to the request at the last possible moment and physically protected. Batch processing requests submitted in punched cards should have the password card added by the user just prior to submission. The computer operations staff should maintain
the card decks in a protected area and should remove and destroy the password card after the deck has been read by the system. The password should never be printed on any output media. One-time passwords that are distributed to the owner in the form of a password list and sequentially used for sequential batch processing requests may be used. The Standard requires that such lists be physically protected by the owner.

Users should be allowed more than one attempt to enter a password correctly in order to allow for inadvertent errors.

However, there should be a maximum number of trials allowed for a password to be entered correctly. A maximum of three (3) attempts is considered adequate for typical users of a computer system. The system should also prevent rapid retries when a password is entered incorrectly. Several seconds should elapse before another password is requested. This prevents an automated, high speed, trial-and-error attack on the password system. A security record should be maintained of the fact that incorrect passwords were entered but the incorrect password should not be kept in the record. A security alarm should be generated if:

- The maximum number of allowed password retries is exceeded;
- The maximum number of allowed failed logons from one terminal is exceeded;
- The maximum number of allowed failed logons for a time period is exceeded.

The system should inform the user, following a successful LOGON procedure, of the last successful access by the user and of any unsuccessful intervening access attempts. This will aid in uncovering any unauthorized accesses or attempted accesses which may have occurred between successful accesses. The user can do several actions to prevent an observer from learning the password by watching the password entry process. First, entry of the password can be practiced so that it can be quickly entered using several fingers. Second, the body can be used to prevent the observer from seeing the keys being pressed during password entry. Third, the user can request that a guest not watch the password entry process. Fourth, the user can perform the password entry prior to demonstrating use of the system.

l) Transmission

Passwords are typically used to authenticate the identity of a user attempting to gain access to a shared computer system or network from a terminal. In order to be authenticated, the password is typically transmitted from the terminal to the computer via the communication line between the terminal and the computer. Unless the communication line is physically protected or encrypted, the password is vulnerable to disclosure. Most communication lines between terminals and computers are not afforded this protection at present. Therefore, users should be aware that their passwords can very easily be disclosed via passive wiretapping.

Computer systems can also be easily spoofed. This can occur if an intruder has inserted an active wiretap between a terminal and the computer. The active wiretap can replace one user's password with another user's password, even if the passwords are encrypted at the terminal. Spoofing occurs when the system is fooled into "believing" one user is at the terminal when another user is actually there. Reverse spoofing occurs when a user is fooled into believing that communication is with the intended computer when another computer is there. In the latter case, an authorized user can be spoofed into providing the valid user's password by simulating the "LOGON" request of the intended computer. After the password is obtained, the intruder that is controlling the spoofing computer informs the user that the requested service is temporarily unavailable. During this exchange the intruder has obtained a valid password without the user's knowledge.

These threats can be prevented by one of two encryption methods. First, the communication line between the terminal and the computer can be protected by encryption devices which use a secret key (e.g., a Data Encrypting Key) for encrypting all communication between the terminal and the computer. Transmitted passwords are thus protected from disclosure. In addition each transmission can be numbered so that a previous transmission cannot replace a later transmission (.i.e., a previously used valid password cannot be saved and used to replace an invalid password, even if both are encrypted). Passwords are thus protected to the same degree as the data as specified IED in the Standard.

Alternatively, the password can be used as the encryption key or as part of the encryption key. Suppose a user enters a password to be used as an encryption key at the terminal (i.e., never transmitted to the computer) and the user's password is retrieved from the computer's memory and used as the encryption key at the computer (i.e., never transmitted to the terminal). Then the terminal and the computer are mutually authenticated if normal communication can occur using the encryption and decryption processes at the terminal and computer, both using the password as the key (or a part of the key). This alternative is also allowed in the Standard.

In order to prevent compromise of the level of security provided by the cryptographic mechanism, the Standard specifies that personal passwords that are used as keys as described above be selected at random from the set of all possible encryption keys used by the cryptographic process. It also specifies that passwords that are used as Data Encrypting Keys should not also be used as Key Encrypting Keys, and vice versa. This is to minimize any possibility of attempting to recover the key (and hence the password) through cryptanalytic techniques.

(a) Authentication Period

Interactive "sessions" between a user and a computer via a remote terminal often last several hours. While security policy should state that a terminal that is "logged onto" a computer should never be left unattended by the user that is "logged onto" the computer, in practice this often occurs. Many systems have a feature which automatically logs a user off the system if the terminal has been inactive for some period of time. This is to prevent someone who encounters an unattended terminal from using it. Some access control systems require that a user be re-authenticated on a periodic basis in addition to the initial authentication process. These systems often antagonize the user if the authentication frequency is set too high. The message that the authentication process must be performed again often comes in the middle of the work that a user is performing. If this work happens to be a large printout of final text of a paper to be published, the user is rightfully upset. For this reason the Standard did not specify a minimum re-authentication period. Re-authentication should only be required to satisfy high security requirements, and then only requested if the terminal has been inactive for a period of time. This should prevent the authentication process from occurring in the middle of some important work.

m) Examples of Password Systems

The following examples of password systems which satisfy various security requirements are provided as assistance to Security Officers and System Managers. Determination of the parameters for each of the 10 factors discussed above will permit the preparation of the Password Standard Compliance Document. These examples should not be considered as the only selection of the parameters for the 10 password system factors.

(1) Password System for Low Protection Requirements

A hypothetical password system might have the following parameters for the 10 factors which will both satisfy the Standard and satisfy requirements for protection which are considered to be minimal. The example is similar to that found in many retail, customer initiated financial transaction systems in which the maximum liability of the customer is $50 and the maximum liability of the bank is limited by the number of transactions allowed per day. This example is also typical of many government-owned, government-leased computer systems in which no sensitive applications are performed. Small scientific systems, special purpose systems and systems not making critical automated decisions may fall in this category. Systems which have limited financial liability and those which require only accountability and control of computer usage and costs may also be considered in this category.

- Length Range: 4-6
- Composition: Digits (0-9)
- Lifetime: l year
- Source: User
- Ownership: Individual (personal password); group (access passwords)
- Distribution: Unmarked envelope in U.S. Mail
- Storage: Central computer on-line storage as plaintext
- Entry: Non-printing "PIN-PAD"
- Transmission: Plaintext
- Authentication Period: Each transaction

(2) Password System for Medium Protection Requirements

Government systems which process limited "sensitive" applications may fall in this category. These are applications which process data leading to or directly related to monetary payments or process data subject to the Privacy Act of 1974. Agency management may determine that additional applications should be designated as sensitive. Computer systems that are subject to fraud, theft, erroneous payments or other loss of sensitive information may also fall into this category. Government systems which make payments (e.g., Social Security, Treasury), keep inventories (e.g., Armed Forces), and process personal information (e.g., Internal Revenue, Service, Department of Education) would be examples of systems which would have requirements of this nature and probably would be satisfIED RET650 by this type of password system.

- Length Range: 4-8
- Composition: U.C. Letters (A-Z), L.C. Letters (a-z), and digits (0-9)
- Lifetime: 6 months
- Source: System generated and user selected
- Ownership: Individual
- Distribution: Terminal and special mailer
- Storage: Encrypted passwords
- Entry: Non-printing keyboard and masked-printing keyboard
- Transmission: Clear text
- Authentication Period: Login and after 10 minutes of terminal inactivity.

(3) Password System for High Protection Requirements

Computer systems which process information of a sensitive nature and which rely on passwords to provide personal identification may have high protection requirements that could be satisfied IED by a password system for personal identification having these characteristics.

Systems having high protection requirement's may include those which have unusually high potential for fraud or theft, have a high economic benefit to a system intruder, and have a substantial impact on safety or the well-being of the society. Some computer systems of the Department of Defense or the Federal Reserve Communication System may fall into this category. Systems having very high security requirements may require methods of personal identification which are based on physical characteristics of a person (signature, voice, fingerprint) or on a combination of something unique that the person has (e.g., badge, ID card) and something unique that the person knows (i.e., a password). A risk analysis should be performed for each government owned or leased computer system to determine its security requirements and then a personal identification system should be selected which best satisfies these requirements.

- Length Range: 6-8

- Composition: Full 95 character set
- Lifetime: One month
- Source: Automated password generator within the authentication system
- Ownership: Individual
- Distribution: Registered mall, receipt required; personal delivery, affidavit required
- Storage: Encrypted passwords
- Entry: Non-printing keyboards
- Transmission: Encrypted communication with message numbering
- Authentication Period: Login and after 5 minutes of terminal inactivity.

4.5 Configuration and Change Control Management

Utilities should have strict procedures and processes in place to control configuration and changes. Access to make changes must be restricted to authorized personnel through the use of change level passwords that aren't common knowledge or factory defaults. Routinely changing passwords for security is a costly and time consuming process but it is highly recommended and should be considered. Access controls or encryption devices in the communication path will be required by regulatory bodies in the future.

Contractors and vendors should never be given the ongoing operating password. Passwords should be changed to a temporary one prior to giving contractors or vendors access to the relays. The passwords should then be changed back or to new ones after the contractors or vendors have completed their work.

4.6 Protection of IED Maintenance Ports

It is well recognized that the dial-up equipment installed to allow remote access to protective relay IED , now protected only by seldom changed passwords, is an undesirable (even unacceptable) vulnerability. One retrofit solution is to install a cryptographic module between the auto-answer modem and the IED whose access is to be protected. Such a module, when used with appropriate hardware/software at the initiating site, would provide authenticated and authorized remote access to the maintenance port, and encryption of the ensuing traffic to thwart eavesdropping. Proof of concept modules to perform this function were demonstrated at two utilities (DTE Energy and Peoples Energy) in 2005 under DoE NETL Project M63SNL34. Functional requirements for these modules and their key management are described in Report AGA 12 Part 1, developed by an industry panel of experts including strong representation from the electric utility industry.

4.7 Physical Security

Unattended facilities like substations are common elements in the electric industry. Substations contain many of the fundamental critical assets necessary for the transmission and distribution of electric power to customers. Transformers, breakers, busses, switches, capacitor banks, Remote Terminal Units (RTUs), Programmable Logic Controllers (PLCs), Intelligent Electronic Devices (IED RET650s), and communication systems can reside within the confines of the substation. The compromise of any one of these elements can impact the integrity of the electric grid, depending on the amount and type of load being served by this substation at the time of the incident.

While the substation is in many ways the “neuron” of the electrical network allowing effective monitoring and control of electric energy in that particular area of the network, they are attended for very short periods of time. Unlike control centers and most power plants that are staffed around the clock, there is typically no staffing, limited or no roving security patrols, and roofed structures are typically designed to protect electronic equipment and switch gear. Typically, substations out number power plants 30:1 and can be located in a downtown setting or in the most remote of rural areas. While most critical substations will logically be located in or near major load centers, interregional ties located in remote substations may be just as critical for interconnection purposes.

Substations are located in urban, suburban, rural, and industrial/commercial sites and the effectiveness of security methods differs greatly from site to site. Because of the diversity in substation size, location, and criticality, each substation should be assessed and classified IED. In general, more rigorous security measures should be applied IED to the more critical substations. While all substations are a critical element in the transmission and distribution of electric energy, not all substations are equally critical to North American electric grid reliability.

This guideline is intended to provide suggestions when considering the physical security at critical substations with a focus on practical methods using existing technology and proven processes. All of the security methods discussed here can be applied IED to existing substations, whether they are critical or not.

Physical security typically comprises five distinct elements, or systems:

- Delay/Deterrence
- Detection
- Assessment
- Communication
- Response

4.8 Remote Access

- Policies and procedures governing use and installation of Remote Access for Electronic Control and Protection Systems, including identifying responsible parties, should be established. These should be reviewed periodically and updated as required.
- Remote Access should only be enabled when required, approved, and authenticated.
- Multi-factor (two or more) authentication should be used. Factors include something “you know” (for example: passwords, destination IP address and/or telephone number), something “you have” (for example: token, digital certificate), something “you are” (for example: biometrics). Other factors may include: source IP address and/or telephone number, GPS location. These will make access more difficult for unauthorized users and will help to ensure identity of authorized Remote Access users.
- Automatically lock accounts or access paths after a preset number of consecutive invalid password attempts. Consider automatically unlocking the account or access path after a pre-determined period of time or by other methods to ensure safe and reliable system operations.

- Encryption should be used when traversing unsecured networks to gain Remote Access. This will help ensure confidentiality and integrity of any information transfer.
- Approved Remote Access authorization lists should be established. These lists should be reviewed periodically and updated as required.
- Change or delete any default passwords or User IDs. Consider using meaningful but non-descriptive IDs.
- All Remote Access enabling hardware and software should be approved and installed in accordance with Policy. The location and specification of Remote Access enabling hardware and software should be documented and maintained in a controlled manner. Periodic audits should be conducted to ensure compliance.
- Remote Access connections should be logged. Logs should be periodically reviewed.
- Consider risk to the process when allowing Remote Access and specifying hardware and software.
- Policy considerations for Remote Access modems:
- Change default settings as appropriate:
- Set dial-out modems to not auto answer.
- Increase ring count before answer.
- Utilize inactivity timeout if available.
- Change passwords periodically.
- Use call back whenever possible.
- Require authentication before connection.
- Make maximum use of available security features.

Exceptions:

- This security guideline does not pertain to real time transfer of data and control commands.
- This security guideline does not address the integrity or confidentiality of the data on the device or of communications to the device.
- This security guideline does not address measures to preserve the availability of the device (i.e., measures to protect against denial of service attacks).

- There may be some legacy Electronic Control and Protection Systems for which it is technically or economically infeasible to apply all of the specifics contained in this security guideline.

4.9 Intrusion Detection Systems (IDS)

Although a strong perimeter defense is vital to securing a control/monitoring network and all its access points, studies show that up to 70% of attacks are internally initiated. Thus, an intrusion detection system (IDS) that looks only at external intrusion attempts is clearly not adequate. The encryption modules described above should include intrusion detection capability for both internal and external attempts to guess passwords or bypass the authentication/authorization functions. Upon detection of an intrusion attempt, the IDS function may shut down further communications through that link or may log the event and report the incident via existing communication links or via an alarm point on an existing SCADA system. Such reporting should ideally go to the person responsible for investigating intrusion attempts, and not to the SCADA operators.

4.10 Recovery/Remedial Action after A Cyber Attack

In the event that a cyber attack is discovered on a relay, it is critical to make a full assessment of the situation as quickly as possible due to the following:

- The incident is unlikely to be an isolated incident
- Left unmitigated, more attacks may occur

Recovery and remediation will require the user to determine five things regarding the attack: Who, What, Where, When, and Why. Depending on the security features of the device and administrative procedures in effect, it may not be possible to determine all of these parameters. In such cases, consideration should be given to upgrading relay technology and installation/maintenance procedures to provide a better analysis of the attack. Without understanding the Who, What, Where, When and Why, it will be very difficult to develop an effective remedial plan to prevent attacks in the future.

- Who

The source of the attack needs to be identified IED to determine how to best prevent future attacks of this nature. If the source is an outside agency without authorized access (direct, or remote) to the relay, technical solutions will be the primary remediation. If, on the other hand, the source is determined to be someone with authorized access to the relay (employee, contractor or authorized third party) procedures such as modification of password policies, background checks, restrictions on laptop/configuration software use may be the key. It is strongly recommended that individual passwords or some other mechanism be employed to determine (or at least or narrow down the list) of who the attacker is. If the technology is not available to determine Who from the device itself, frequently the other parameters, when determined, will provide some insight to the attacker's identity. Of paramount concern will be the situation where the attacker is identified IED as an employee, contractor or authorized third party. In such case, the user will need to consider any other sites that the attacker had access to and inspect for other similar activity.

- What

What the attack was, or in other words, the nature of the attack, needs to be thoroughly analyzed. The type of attack will have a major impact on the recovery and remediation of the attack. For example:

  - If data theft (e.g., configuration upload) has occurred, the user must consider if passwords have been compromised. Personnel will typically reuse passwords for similar applications and the compromising of those passwords creates a larger issue within the user's environment. Recovery in this instance may include the wholesale change of all protective relay and configuration software passwords.
  - If settings have been changed to render faulty operation, the user should look to similar devices to see if changes have been made there as well.

Also, the nature of the change may provide a clue to the source. Subtle changes, such as raising/lowering target values may indicate a person with specific knowledge about the user’s facilities and perhaps access to the device‘s configuration software. Badly corrupted configurations or blindly operated points which are easily detected may suggest an outside hacker.

- Where

Where the attack took place is a two-fold question; where in terms of the location of the asset (e.g., substation location) and where in the substation (which relay(s), communications processors, dialers, et. al).

Identifying the substation itself may be important if the attack is determined to be from a threat with access to the station. If the threat is traced to a contractor, for example, all stations in which the contractor had access will need to be evaluated for the possibility that they too have been attacked. Attacks which are limited to a geographical area will similarly help to identify which personnel may be involved.

The other aspect is which relays or other devices in the protective relaying scheme have been attacked. Important to determine are the brand, model, firmware version of the device attacked to provide further clues on both the nature of the attack and the probability of widespread attack elsewhere on the system. Benefits of this information include:

- Gaps in security for various products can be brought to the vendor’s attention for technical remediation.
- Vulnerable devices can be removed from the system or restricted in access by procedural means.
- Inspection of other substations can be more easily facilitated if the user knows where to look (which relays) and what to look for.

- When

When the attack took place can be an important tool in determining WHO. Knowing when can allow the user to co-relate the attack with authorized personnel movement and work shifts, vendor and contractor site activities, hacker activity (e.g. attacks occurring from another time zone).

The attacks may also be correlated to other activities and procedures such as the installation of new firmware, password changes, employment changes, labor disputes/negotiations, activities, (internally and externally), communication system changes.

- Why

Though not a technical issue per se, WHY an attack took place is an important step in the prevention of future attacks. Hackers and outside agents attack for gratification and to further their causes, and little be done other than to harden assets from a technical nature and assist law enforcement with the apprehension of those responsible. But attacks generated by disgruntled employees, contractors, or vendors are the most difficult to detect/prevent and consideration must be given to preventing situations which would cause someone to seek redress through this method. Correlation of such attacks to cause can be useful in the prevention of future attacks. Users can and should monitor the temperament of any personnel (internal, contractors, vendors, system integrators) who could launch such an attack and address concerns before they lead to cyber attacks, or escalate security measures in the event that confrontation is expected.

4.11 Final Recommendation

As normally said that security is everyone responsibility and it is not just limited to technical solution, it is about the culture and processes adopted in an organization. Figure 4.2 shows a comprehensive view of security that covers it all.

- Establish a broad corporate security policy based on its recommendations, tailored to the needs of protective relay systems
- Assess existing communications channels for vulnerabilities to intrusion

- Implement and enforce policies re computer usage, remote access control, with frequent auditing of systems and policies. Emphasize that security is not a part time ad hoc function. Have certain people in the utility be accountable for security (not IT, or not IT only)
- Where appropriate, add policies, procedures and hardware (cryptographic modules) to vulnerable communications channels and access ports.
- Monitor logs – see what is happening to the equipment/system
- Monitor traffic – who is getting access
- Maintain and monitor a list of authorized personnel who have password or authenticated access

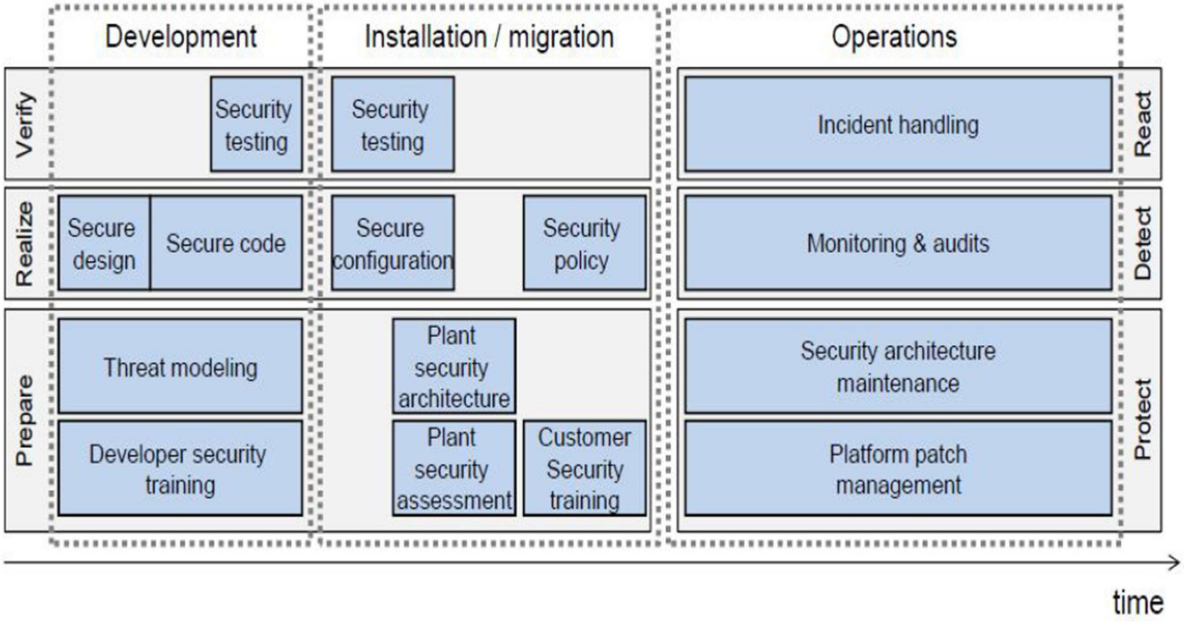


Fig 4.2. A Comprehensive View of Security

The following section recommends selected aspects of the various means of protecting systems. These means include:

- Physical protection ("guards and gates"). This is always a consideration. Where possible, physical protection should always be provided. Many attacks are simplified IED by physical access to equipment. However, in electric power systems there are numerous situations under which physical protection is difficult or impossible, including equipment located on customer premises or in small, remote substations.

- Isolation. This is the traditional means of information security protection. For communications, it has sometimes been called “air gap security.” Isolation usually requires physical protection, with both physical and electronic access limited to a small group of trusted individuals.
- Access control. This is the mediation of access by security functionality within the system. Isolation can be considered a very coarse form of access control, and finer-grained access control is usually required even in isolated systems to prevent inadvertent errors and to provide protection if one of the trusted individuals is compromised.
- Logging and auditing. Logging security-relevant activity and auditing the logs can be used as a means of detecting and deterring malicious activity. In some cases, it is inadvisable to prevent access, such as in emergencies where arrangement of proper access authorization may be difficult. However, malicious activity can be deterred by logging emergency activity and auditing the logs for suspicious situations. Intrusion detection can be regarded as a form of real-time auditing.
- Encryption. This technology has many important uses in protective systems.
- “Security Through Obscurity” is not a valid protection. The notion that obscure technology is protective is a common misconception that is frequently attacked by security experts. Indeed, a fundamental principle in encryption systems is due to Kerckhoffs who stated in 1883 that a system should remain secure even when the adversary has all the information about its operation other than secrets such as passwords and encryption keys.

Chapter 5: Engineering and Configuration of Transformer Protection IED RET650

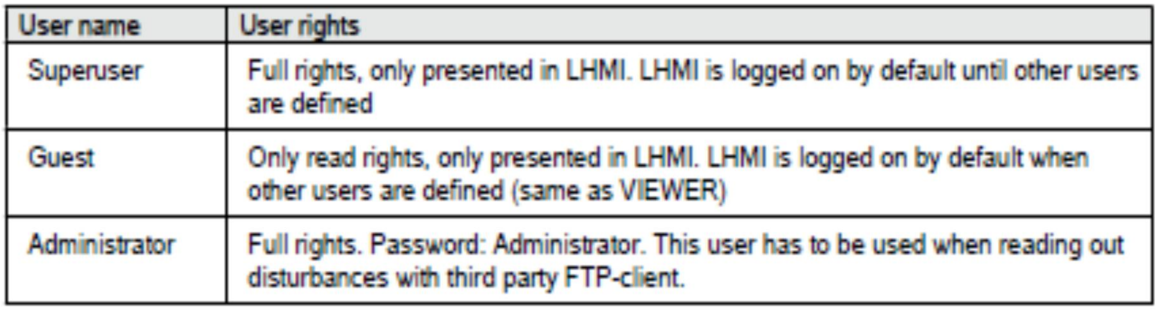
In this chapter, we will engineer and configure a transformer protection IED RET650 (ABB RET650) for a real life substation environment. At the end, we will critically evaluate this IED RET650 for its compliance to IEEE standard for Cyber Security.

The implementation of Cyber Security standards has following aspects [18]:

1. RBAC (Role Based Access Control)
2. Secure System Setup
3. Activity Logs
4. Human Machine Interface

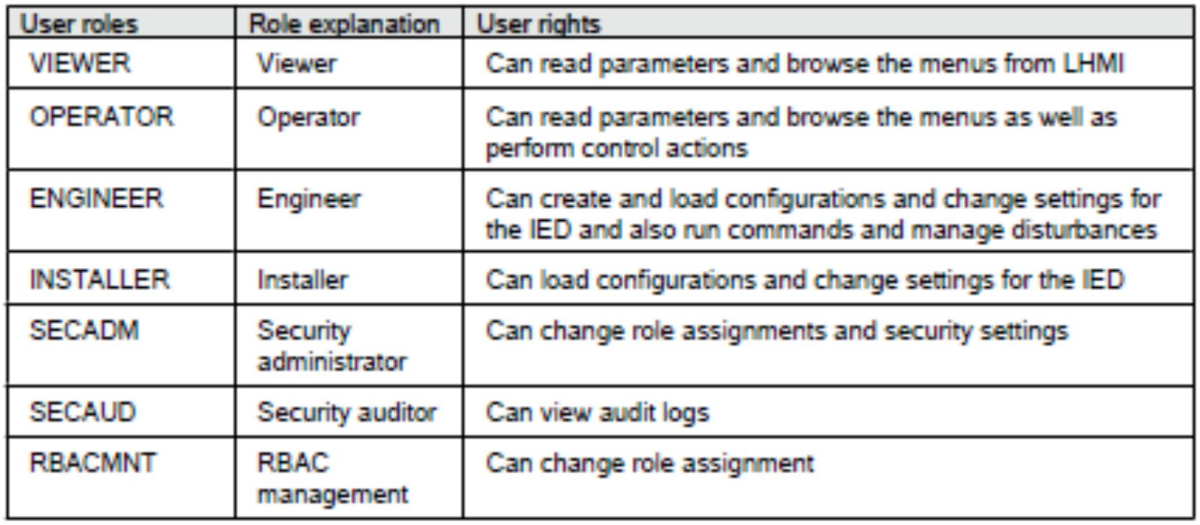
5.1 Role Based Access Control

At the time of initial setup, the IED RET650 has the access rights of “SuperUser” by default. We will change them as per our project requirement by using PCM600 User Management Software Tool [21]. The pre-defined users and their roles are given below in table 4 and 5.



User name	User rights
Superuser	Full rights, only presented in LHMI. LHMI is logged on by default until other users are defined
Guest	Only read rights, only presented in LHMI. LHMI is logged on by default when other users are defined (same as VIEWER)
Administrator	Full rights. Password: Administrator. This user has to be used when reading out disturbances with third party FTP-client.

Table 4 Pre-defined User Names

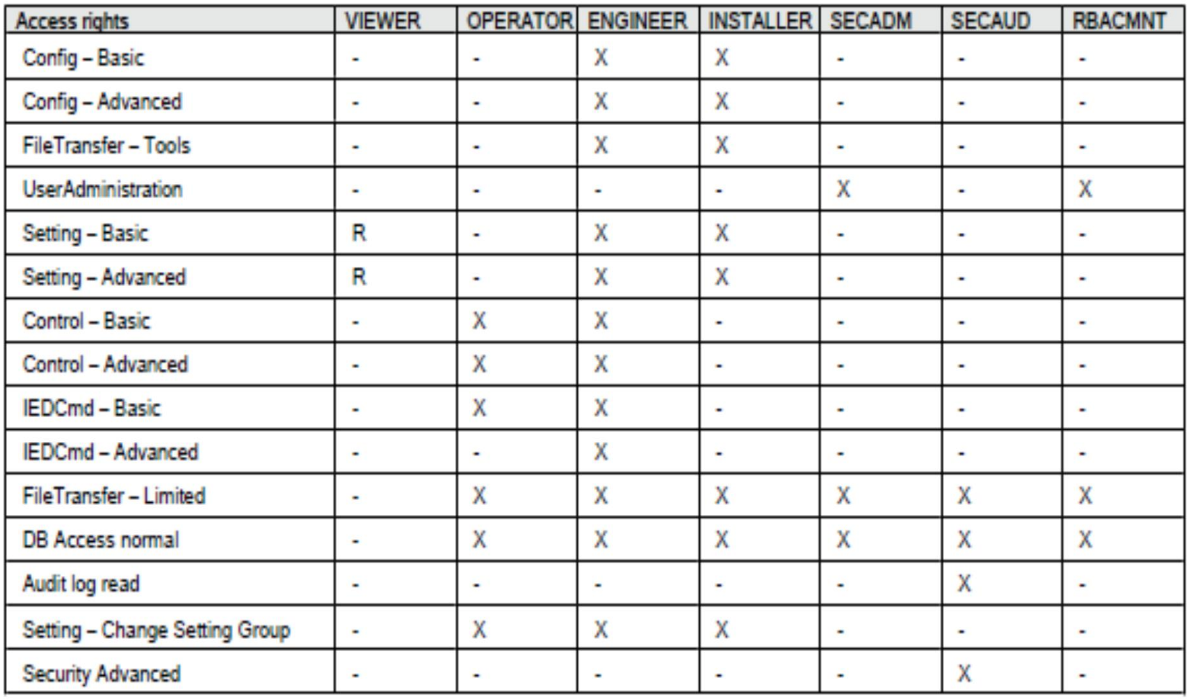


User roles	Role explanation	User rights
VIEWER	Viewer	Can read parameters and browse the menus from LHMI
OPERATOR	Operator	Can read parameters and browse the menus as well as perform control actions
ENGINEER	Engineer	Can create and load configurations and change settings for the IED and also run commands and manage disturbances
INSTALLER	Installer	Can load configurations and change settings for the IED
SECADM	Security administrator	Can change role assignments and security settings
SECAUD	Security auditor	Can view audit logs
RBACMNT	RBAC management	Can change role assignment

Table 5 Pre-defined User Roles

The access rights are defined in the following table no. 6.

X=Full Access rights R=Read Only - =No access rights



Access rights	VIEWER	OPERATOR	ENGINEER	INSTALLER	SECADM	SECAUD	RBACMNT
Config – Basic	-	-	X	X	-	-	-
Config – Advanced	-	-	X	X	-	-	-
FileTransfer – Tools	-	-	X	X	-	-	-
UserAdministration	-	-	-	-	X	-	X
Setting – Basic	R	-	X	X	-	-	-
Setting – Advanced	R	-	X	X	-	-	-
Control – Basic	-	X	X	-	-	-	-
Control – Advanced	-	X	X	-	-	-	-
IEDCmd – Basic	-	X	X	-	-	-	-
IEDCmd – Advanced	-	-	X	-	-	-	-
FileTransfer – Limited	-	X	X	X	X	X	X
DB Access normal	-	X	X	X	X	X	X
Audit log read	-	-	-	-	-	X	-
Setting – Change Setting Group	-	X	X	X	-	-	-
Security Advanced	-	-	-	-	-	X	-

Table 6 Access Rights

IED RET650 users can be created, deleted and edited only with the IED RET650 User Tool within PCM600. Logging on or off can only be done on the local HMI on the IED RET650, there are no users, roles or rights that can be defined on local HMI.

Default User ID: Administrator

Password: Administrator

There are certain restrictions for choosing user names like characters A-Z and 0-9 can be used irrespective of the case sensitivity. First user created must be with the role SECADM (security administrator) to be able to write users created in PCM600 to the IED RET650.

In order to allow the IED RET650 to communicate with PCM600 when users are defined via the IED RET650 Users tool, the access rights “UserAdministration” and “FileTransfer — Limited” must be 72pplied RET650 to at least one user.

5.1.1 Password Policy in IED RET650

Only ASCII characters are allowed when typing username or password. Currently passwords in the range 32-126 and 192-383 (ASCII ranges, decimal) are supported. Password policies are set in the IED RET650 Users tool in PCM600. There are several options for forcing the password safer. To achieve IEEE 1686 standard conformity, a password with minimum length of 8 characters must be used.

- Minimum length of password (1 – 12)
- Require lowercase letters (a – z)
- Require uppercase letters (A – Z)
- Require numeric letters (0 – 9)
- Require special characters (!@#+”*%&/=?)

5.1.2 Starting User Management Tool

Following steps need to be done to access the PCM600 User management tool:

Connect the PC to the IED RET650
Start PCM600

Select an IED RET650 in the object tree

Select Tools/IED RET650 Users or,

Right-click an IED RET650 in the object tree and select IED RET650 Users

Once we follow the above steps, following screen will appear. We can see in Figure 5.1 that a project in the name of **Ryerson University** is already created, with substation, voltage level, bay and then RET650 IED RET650 has been inserted. The application configuration drawings are also attached with this project report for details regarding engineering of this device.

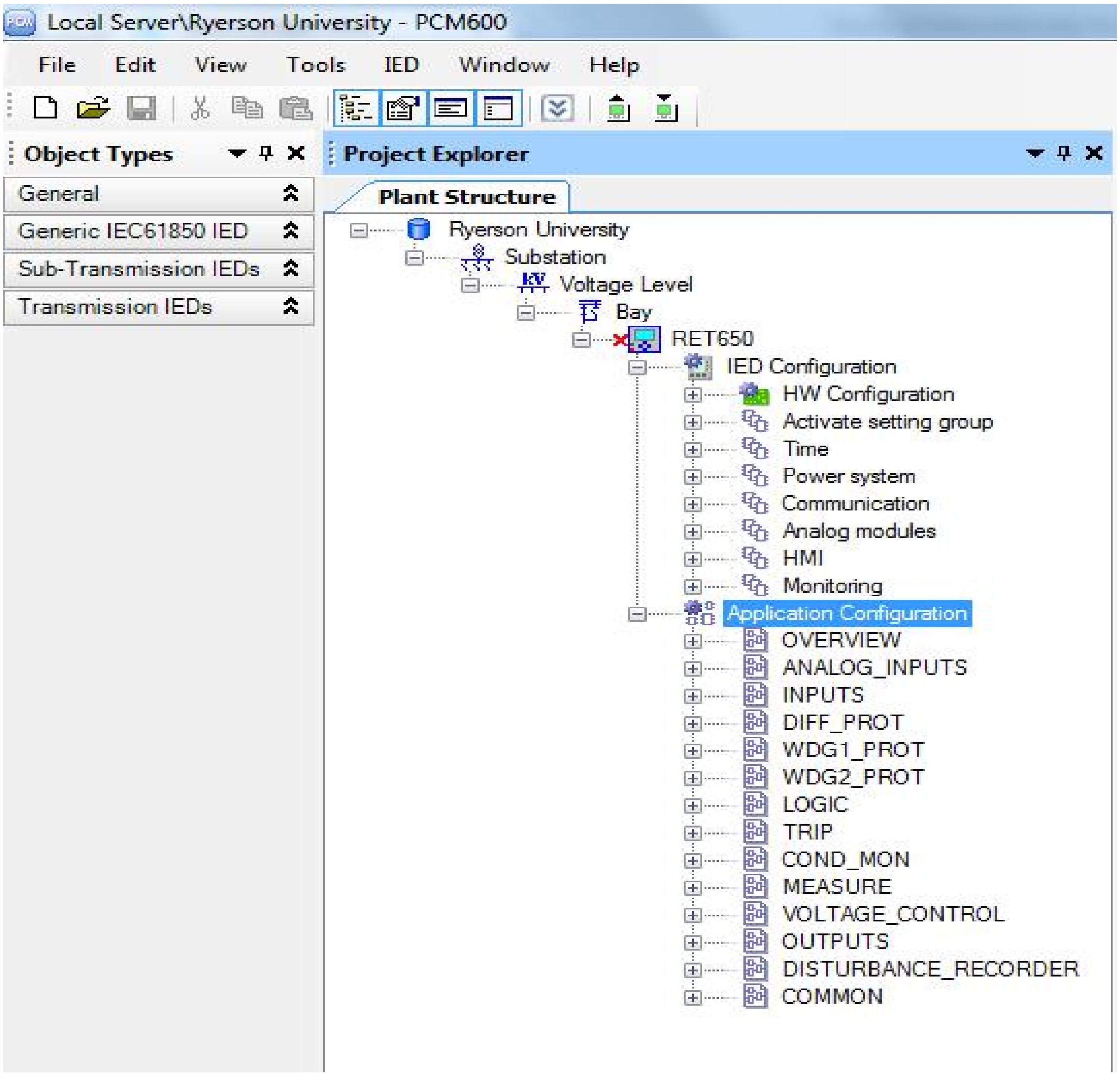
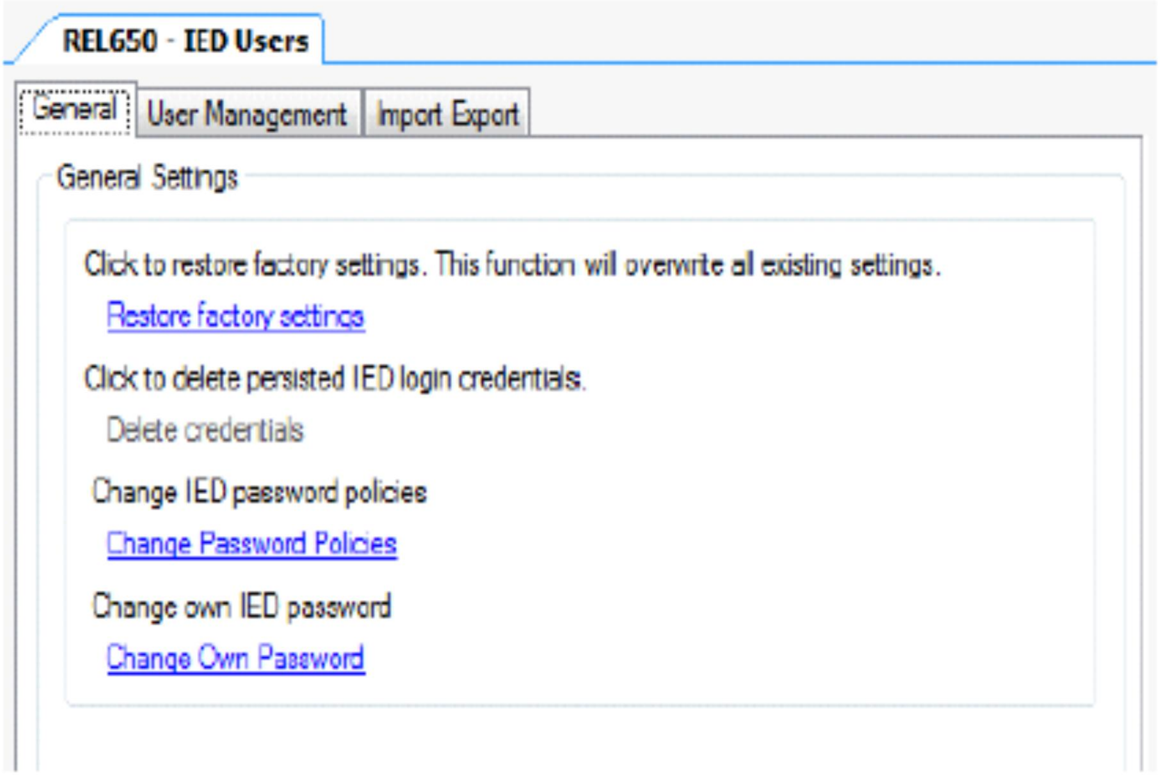


Fig 5.1 PCM600 Ryerson Project Structure

Once we start the PCM600 User tool, we will see the following screen shown in Figure 5.2.


REL650 - IED Users

General Settings

Click to restore factory settings. This function will overwrite all existing settings.

Restore factory settings

Click to delete persisted IED login credentials.

Delete credentials

Change IED password policies

Change Password Policies

Change own IED password

Change Own Password

Fig 5.2 PCM600 User Management Tool

In the General tab, by clicking Restore factory settings the default users can be restored in the IED RET650 Users tool. This means reverting back to the factory delivered users. Performing this operation does not remove the users in the IED RET650. Nothing is changed in the IED RET650 until a "writing-to-IED RET650 operation" is performed.

In the User Management tab, the user profiles of the selected IED RET650 can be edited. New users can be created, existing users can be deleted and different user group members can be edited, as shown in Figure 5.3 below.

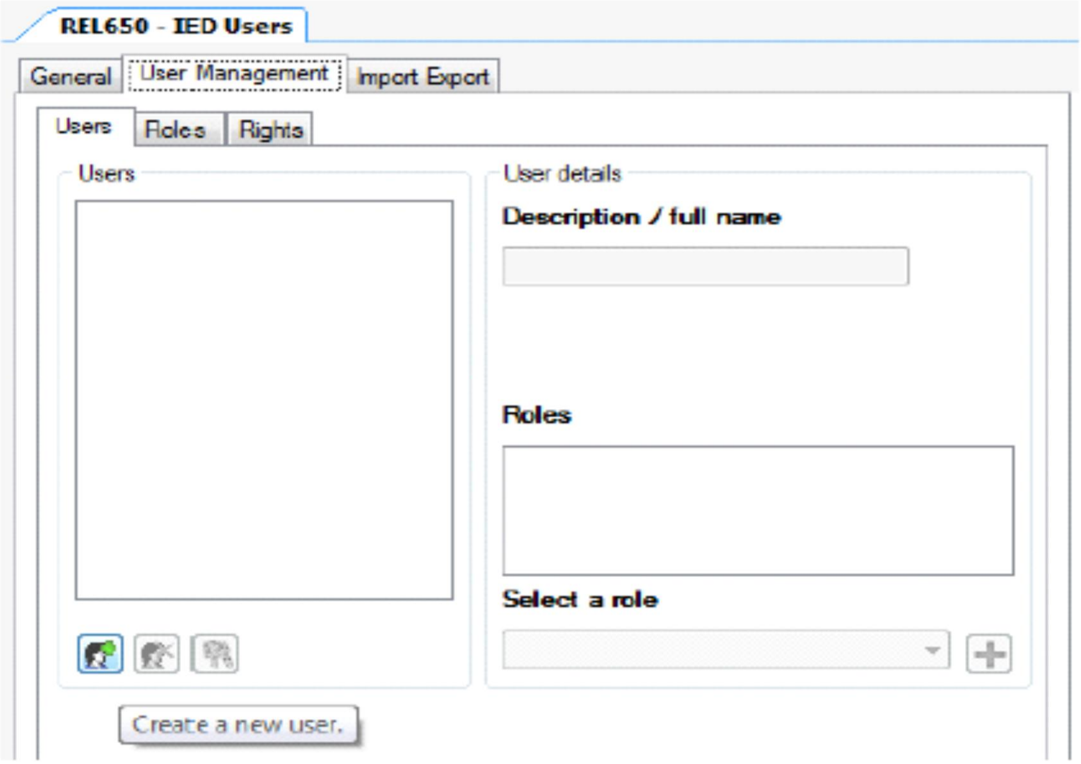
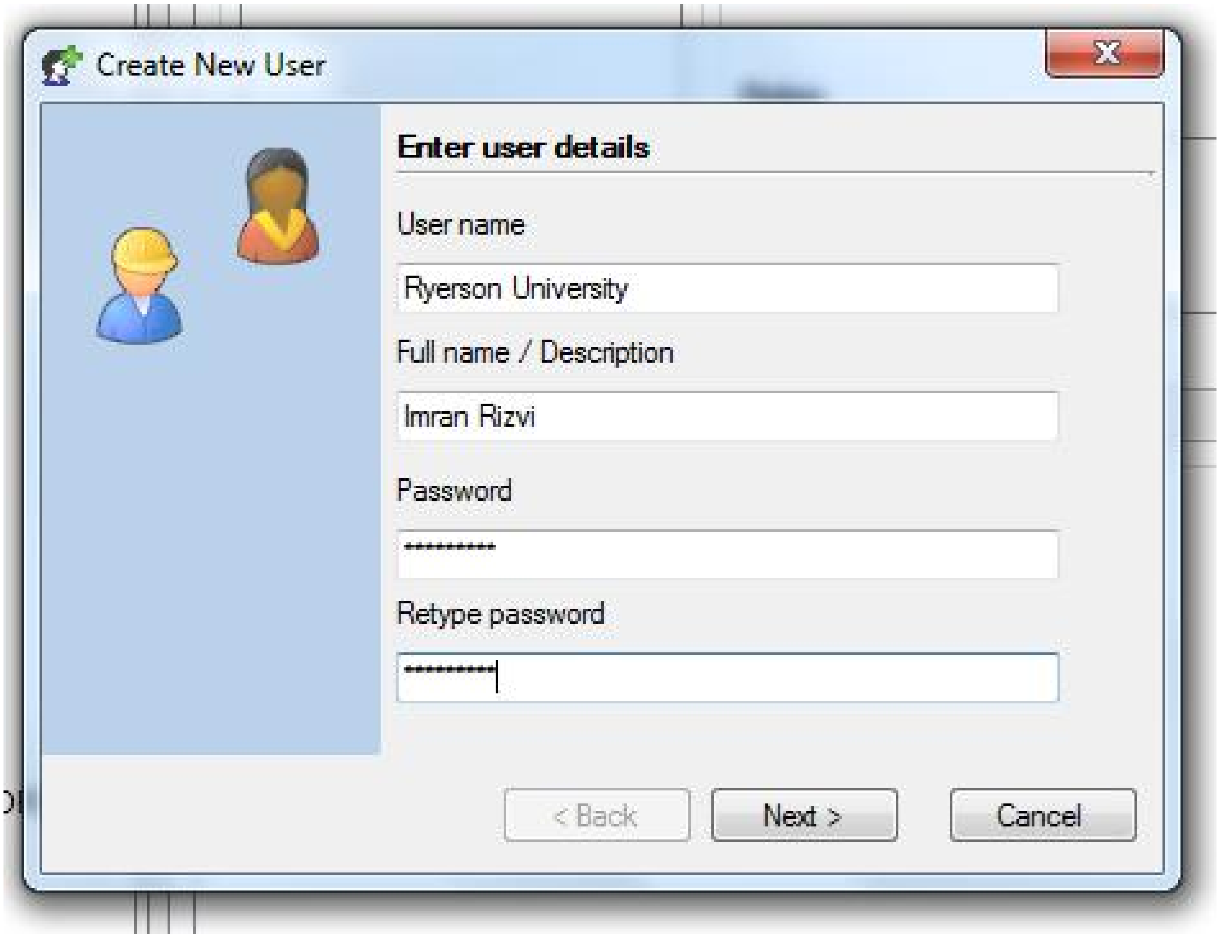


Fig 5.3 PCM600 Adding new User

For this project, we have taken the following credentials:

User name: Ryerson University
Full Name: Imran Rizvi
Password: XXXXXXXXX

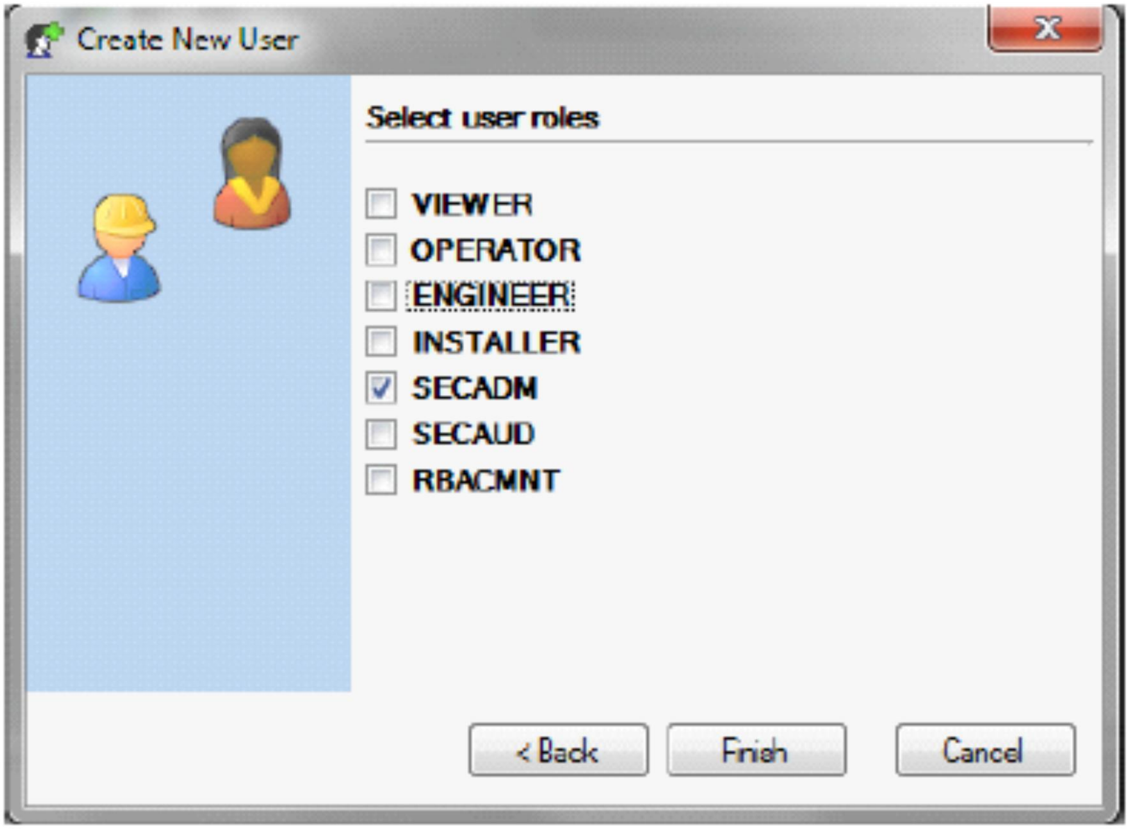
Please see the screen shot below in Figure 5.4.



User name
Ryerson University
Full name / Description
Imran Rizvi
Password
****
Retype password
****

Fig 5.4 Defining User Name and Password

Follow the instructions in the wizard to define a user name, password and user group. Select at least one user group where the defined user belongs. The user profile can be seen in the User details field. As mentioned earlier, the first user has to be a SECADM (Security Administrator). Please see the screen shot below in Figure 5.5.



Create New User

Select user roles

☐ VIEWER
☐ OPERATOR
☐ ENGINEER
☐ INSTALLER
☑ SECADM
☐ SECAUD
☐ RBACMNT

Fig 5.5 Defining User Role

By hitting the finish button, a new user has been created. Additional users can be created by repeating the above procedure. Passwords for any user can also be changed by hitting the password change icon in the figure 5.6 below.

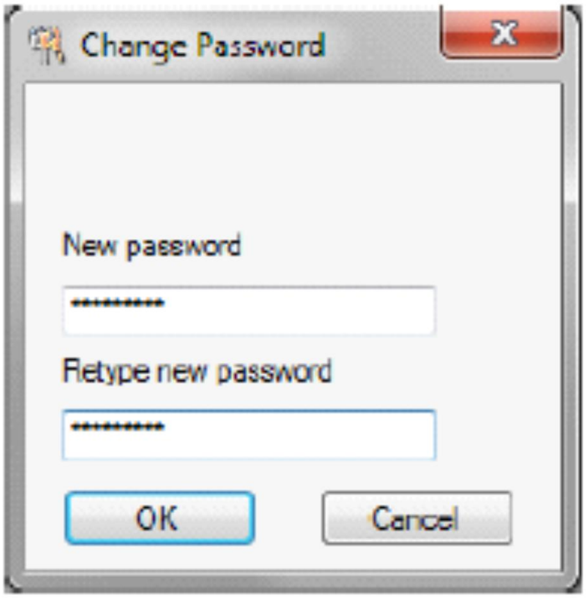
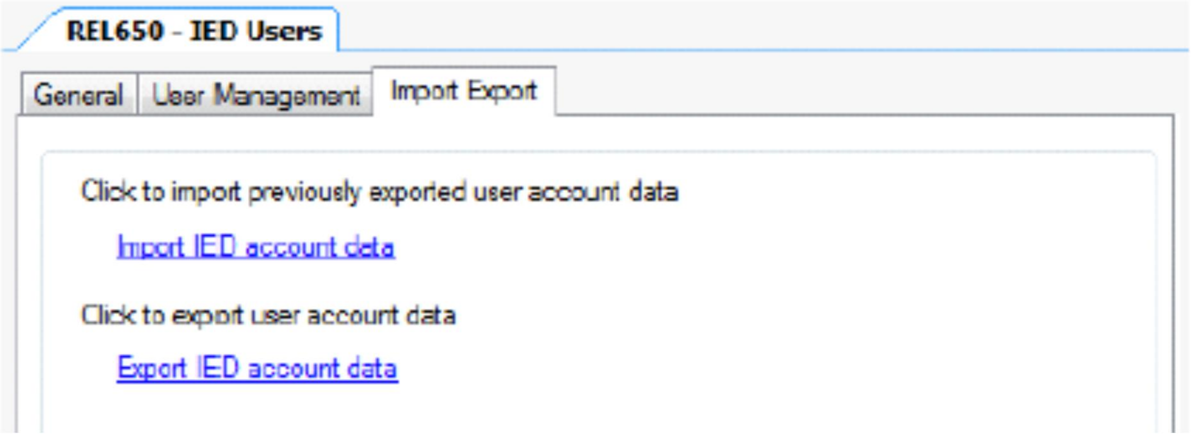


Fig 5.6 Changing Passwords

In real life substation environment, the users and their roles are defined in any organization. So, we can just export the complete user management data from another IED and then import it into the IED RET650 which is being configured for this project. This is done by using the tab "Import Export" as shown in the following screen shot, Figure 5.7.

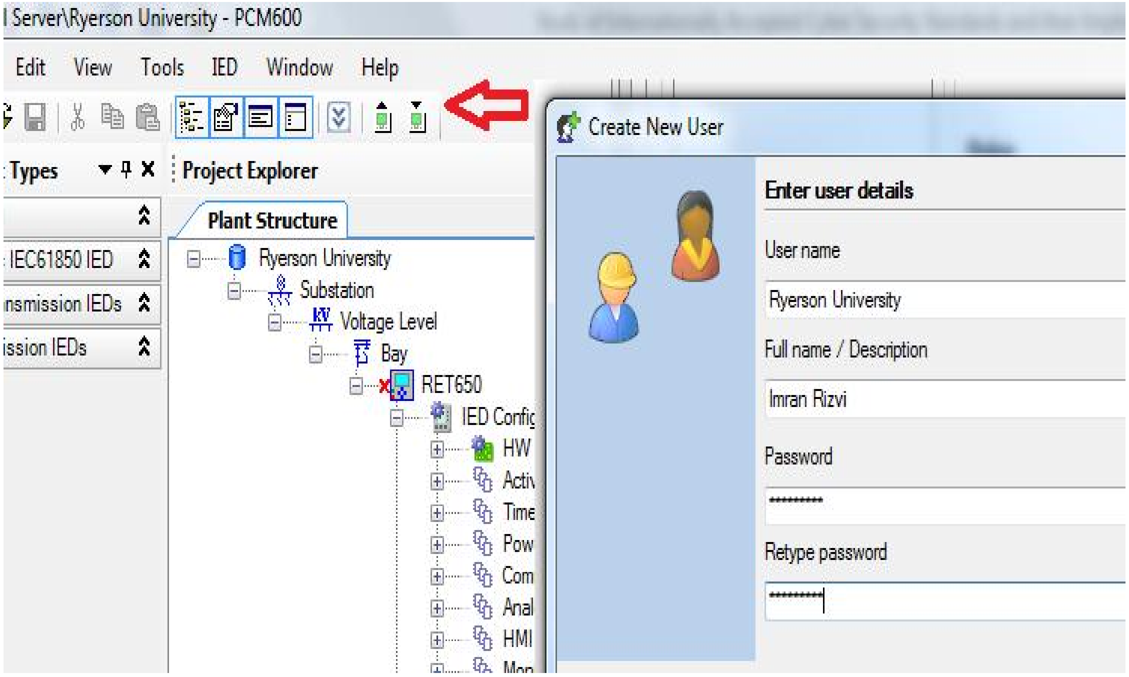


Click to import previously exported user account data

Click to export user account data

Fig 5.7 Importing/Exporting User Management Data

The next step is to download this configuration to the relay. This is done by pressing the icon indicated in RED below in Figure 5.8.



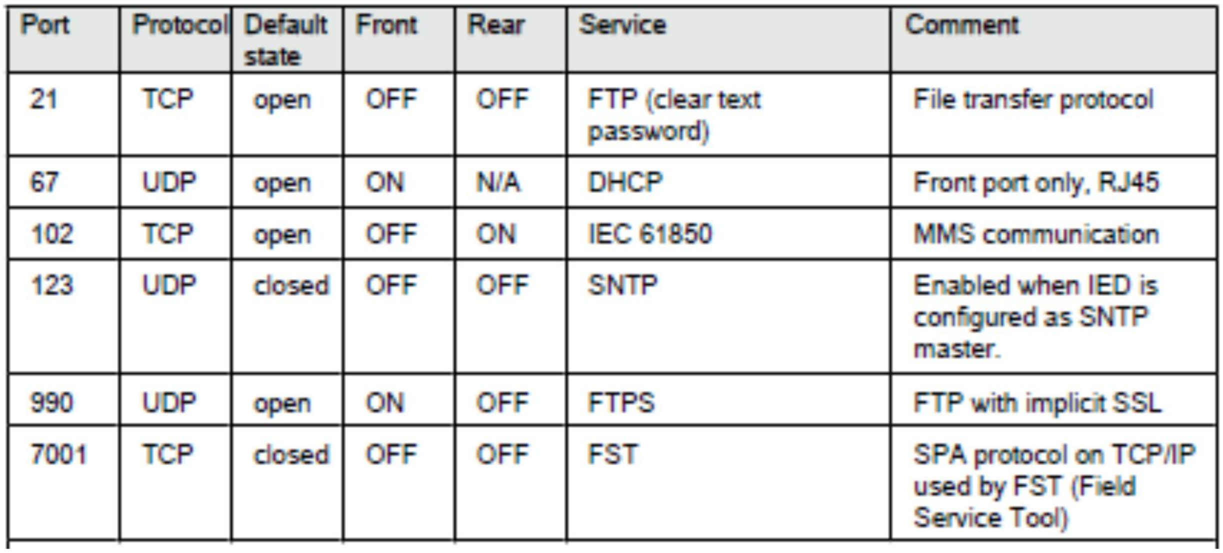
User name: Ryerson University
Full name / Description: Imran Rizvi
Password: *********
Retype password: *********

Fig 5.8 Downloading Data into IED RET650

5.2 Secure System Setup:

To reduce exposure for cyber-attacks and thus comply with cyber security requirements, it must be possible to prevent services in the IED RET650 from operating on other physical interfaces than the ones specified by the vendor or by the owner.

The IP port security guideline cannot suggest concrete products for a secure system setup. This must be decided within the specific project, requirements and existing infrastructure. The required external equipment can be separate devices or devices that combine firewall, router and secure VPN functionality. To set up an IP firewall the following table 7 summarizes the IP ports used in this IED RET650. The ports are listed in ascending order. The column "Default state" defines whether a port is open or closed by default. All ports that are closed can be opened as described in the comment column in the table. Front and Rear refer to the physical front and rear ports. The protocol availability on these ports is configurable.



Port	Protocol	Default state	Front	Rear	Service	Comment
21	TCP	open	OFF	OFF	FTP (clear text password)	File transfer protocol
67	UDP	open	ON	N/A	DHCP	Front port only, RJ45
102	TCP	open	OFF	ON	IEC 61850	MMS communication
123	UDP	closed	OFF	OFF	SNTP	Enabled when IED is configured as SNTP master.
990	UDP	open	ON	OFF	FTPS	FTP with implicit SSL
7001	TCP	closed	OFF	OFF	FST	SPA protocol on TCP/IP used by FST (Field Service Tool)

Table 7 Available IP Ports

The IED RET650 supports two Ethernet communication protocols, which are IEC 61850 and DNP3.0. These communication protocols are enabled by configuration. This means that the IP port is closed and unavailable if the configuration of the 650 series does not contain a communication line of the protocol. If a protocol is configured, the corresponding IP port is open all the time.

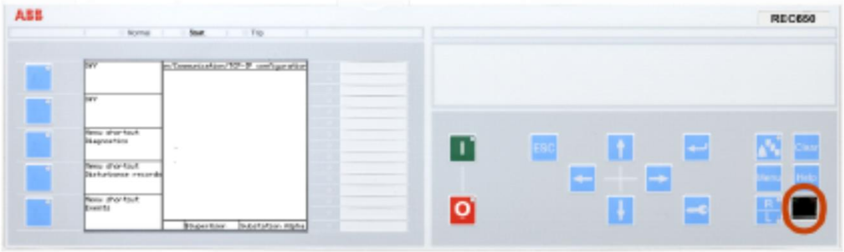
There are some restrictions and dependencies:

- The IP port used for DHCP (default UDP port 67) between the IED RET650 and a computer is fixed and cannot be changed.
- The IP port used for IEC 61850 (default TCP port 102) is fixed and cannot be changed.
- The IP ports used for DNP3 are configurable. The communication protocol DNP3 could operate on UDP (default port 20 000) or TCP (default port 20 000). It is defined in the configuration which type of Ethernet communication is used. Only one type is possible at a time.
- The IP port used for FTP (default TCP port 21) can be changed in the IED RET650 if needed by a 3rd party FTP client.

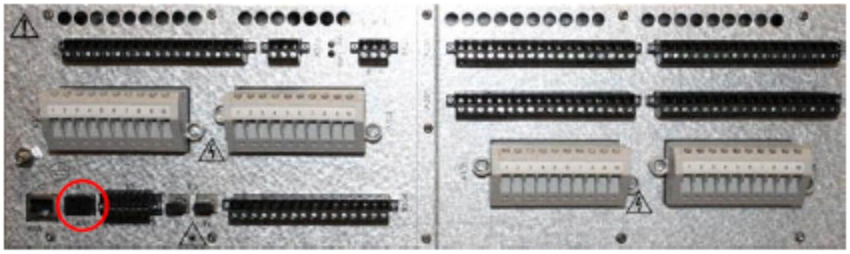
Two ports are used by PCM600. For configuration and parameter settings, the IP port for a proprietary ODBC protocol is used (TCP port 2102) and the port is fixed and cannot be changed. For Field service tool, the IP port for a proprietary SPA protocol is used (TCP port 7001) and the port is fixed and cannot be changed. IP routing is not possible via any of the physical interfaces. Some IP ports are not possible to use in all physical interfaces.

Figure 5.9 shows several interfaces options available in RET650.

For example, the front Ethernet port used for PCM600 is shown in the following picture with red circle.



The rear Ethernet port LAN1 is shown in the red circle



Rear Ethernet ports LAN1A and LAN1B are shown below:

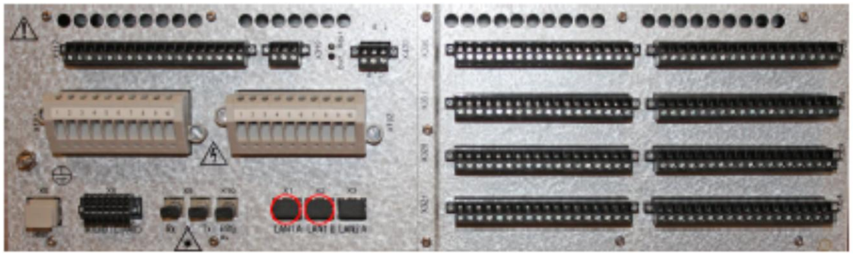


Fig 5.9 Communication Interfaces on Front/ Rear Sides of IED RET650

5.2. FTP Access with SSL:

The FTP Client defaults to the best possible security mode when trying to negotiate with SSL. The automatic negotiation mode acts on port number and server features. It tries to immediately activate implicit SSL if the specified RET650 port is 990. If the specified RET650 port is any other, it tries to negotiate with explicit SSL via AUTH SSL/TLS. Using FTP without SSL encryption gives the FTP client reduced capabilities. This mode is only for accessing disturbance recorder data from the IED RET650.

5.3 Encryption Algorithms:

SSL/TLS connections are encrypted with AES 256 if possible or AES 128 as a minimum. At startup a negotiation decides between these two options. No passwords are stored in clear text within the IED RET650. An encrypted representation of the passwords with SHA 256 is stored in the IED RET650. These are not accessible from outside via any ports.

5.4 Denial of Service Functionality:

The denial of service function is designed to limit the CPU load that can be produced by the Ethernet network traffic on the IED RET650. The communication facilities must not be allowed to compromise the primary functionality of the device. All inbound network traffic is quota controlled, so that a too heavy network load can be controlled. Heavy network load might for instance be the result of malfunctioning equipment connected to the network. The denial of service functions DOSFRNT, DOSLAN1 measure the IED RET650 load from communication and, if necessary, limits it from jeopardizing the IED RET650's control and protection functionality due to a high CPU load. The function has the following outputs:

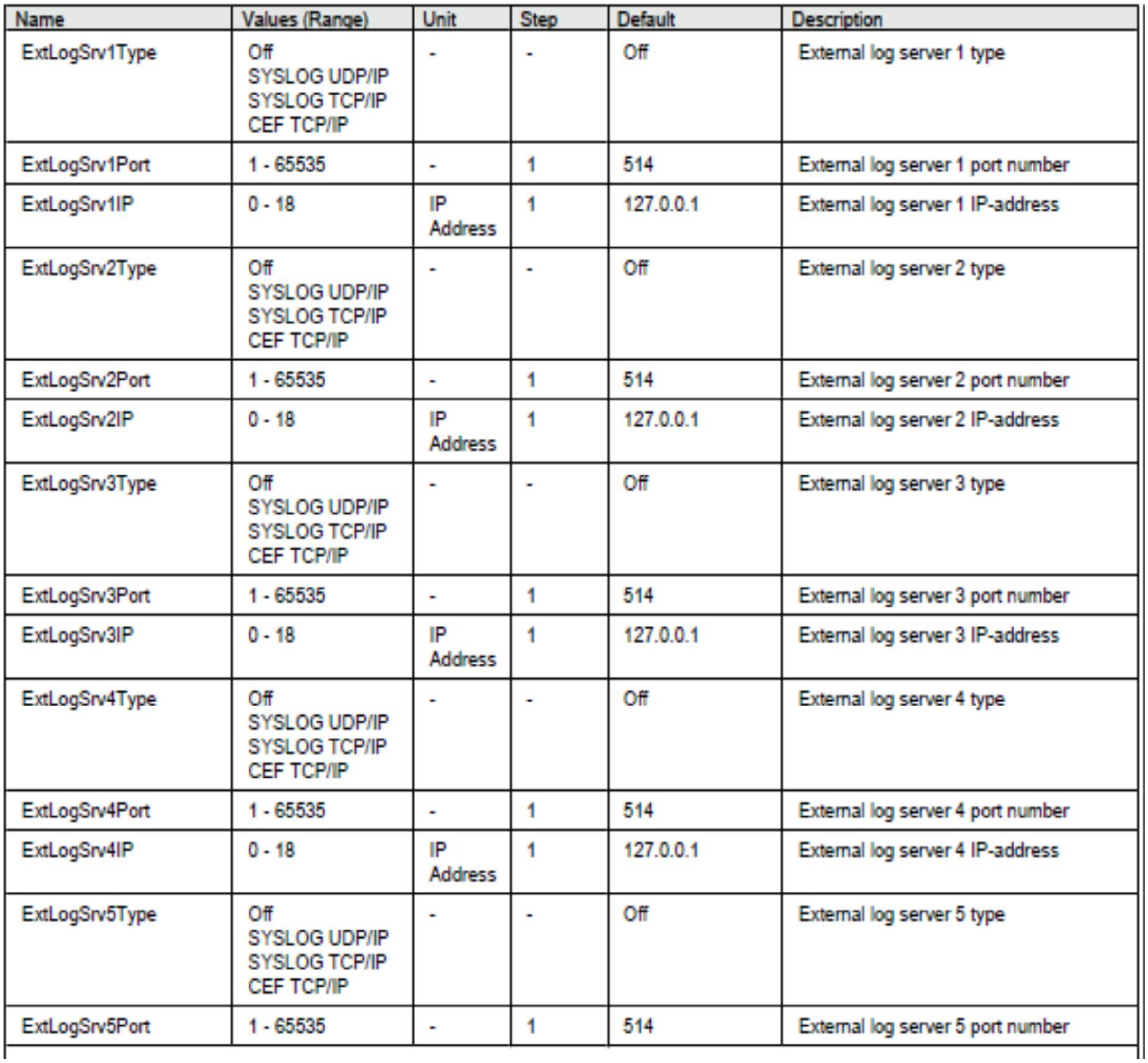
- LINKUP indicates the Ethernet link status
- WARNING indicates that the data rate is higher than 3000 frames/s
- ALARM indicates that the IED RET650 limits the IP-communication

5.5 Certificate Handling:

A self-signed certificate is signed by the IED RET650 it certifies. Certificates use encryption to provide secure communication over the network. Certificate encryption strength depends on the certificate authority (CA). The certificate is always trusted during communication between the IED RET650 and PCM600. If Windows is configured to use UAC High the certificate have to be manually trusted in a dialog box.

5.6 User Activity Logging:

The logic node ACTIVLOG contains all settings for activity logging. There can be 6 external log servers to send syslog events to. Each server can be configured with IP address; IP port number and protocol format. The format can be either syslog (RFC 5424) or Common Event Format (CEF) from ArcSight. Some of the settings related to activity logging is given below in table 8 for reference purposes.



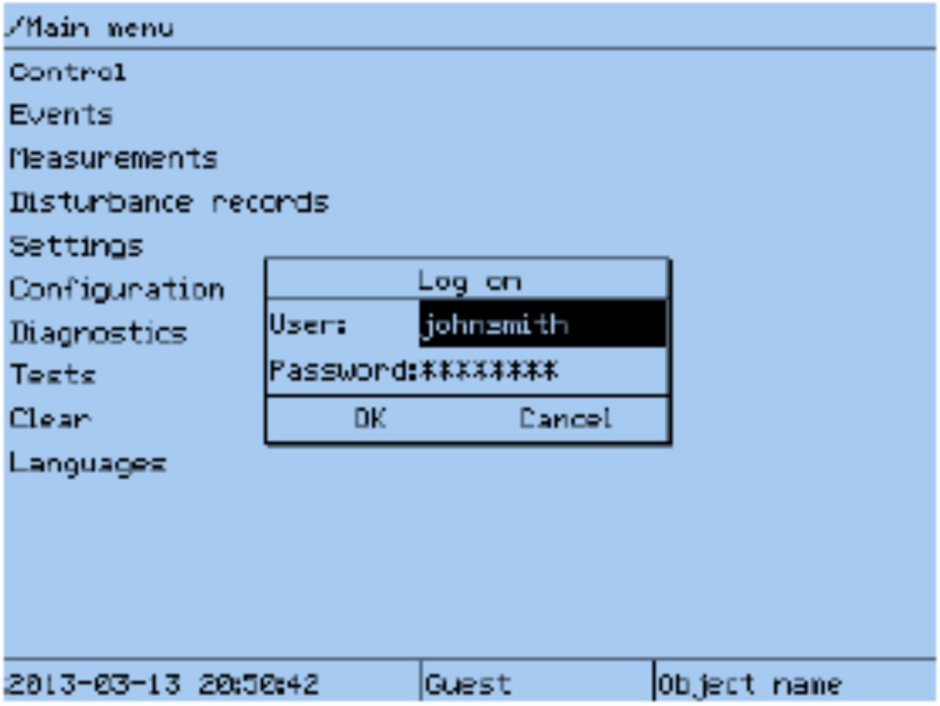
Name	Values (Range)	Unit	Step	Default	Description
ExtLogSrv1Type	Off SYSLOG UDP/IP SYSLOG TCP/IP CEF TCP/IP	-	-	Off	External log server 1 type
ExtLogSrv1Port	1 - 65535	-	1	514	External log server 1 port number
ExtLogSrv1IP	0 - 18	IP Address	1	127.0.0.1	External log server 1 IP-address
ExtLogSrv2Type	Off SYSLOG UDP/IP SYSLOG TCP/IP CEF TCP/IP	-	-	Off	External log server 2 type
ExtLogSrv2Port	1 - 65535	-	1	514	External log server 2 port number
ExtLogSrv2IP	0 - 18	IP Address	1	127.0.0.1	External log server 2 IP-address
ExtLogSrv3Type	Off SYSLOG UDP/IP SYSLOG TCP/IP CEF TCP/IP	-	-	Off	External log server 3 type
ExtLogSrv3Port	1 - 65535	-	1	514	External log server 3 port number
ExtLogSrv3IP	0 - 18	IP Address	1	127.0.0.1	External log server 3 IP-address
ExtLogSrv4Type	Off SYSLOG UDP/IP SYSLOG TCP/IP CEF TCP/IP	-	-	Off	External log server 4 type
ExtLogSrv4Port	1 - 65535	-	1	514	External log server 4 port number
ExtLogSrv4IP	0 - 18	IP Address	1	127.0.0.1	External log server 4 IP-address
ExtLogSrv5Type	Off SYSLOG UDP/IP SYSLOG TCP/IP CEF TCP/IP	-	-	Off	External log server 5 type
ExtLogSrv5Port	1 - 65535	-	1	514	External log server 5 port number

Table 8 Activity Log Settings

5.7 Local Human Machine Interface:

Local HMI, as shown in Figure 5.10, is normally used for day to day operations in the substation to retrieve the fault data and read the settings. This is done without the use of password. Other functions like changing settings, configuration/ engineering and local controls requires password and proper log in. Following steps need to be followed to access such information and commands. To access this functionality, we need to follow the steps below:

Press the "key" button on the LHMI to activate the logon procedure.
The logon is also activated when attempting a password-protected operation.
Select the user name by scrolling up and down keys on the LHMI, and then enter the password by using the same up and down keys as shown in the following screen shot:



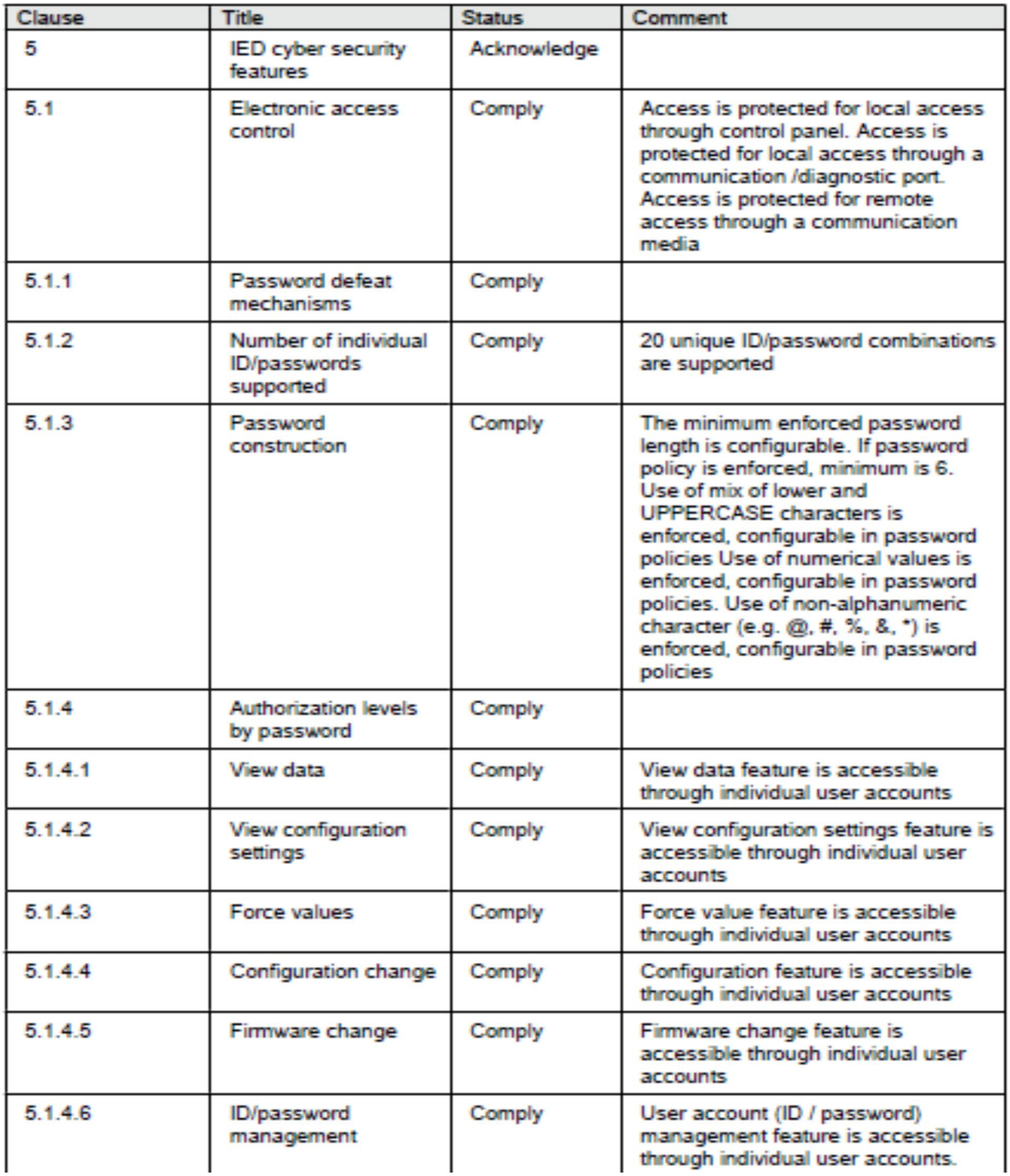
User: johnsmith
Password:********

2013-03-13 20:50:42 | Guest | Object name

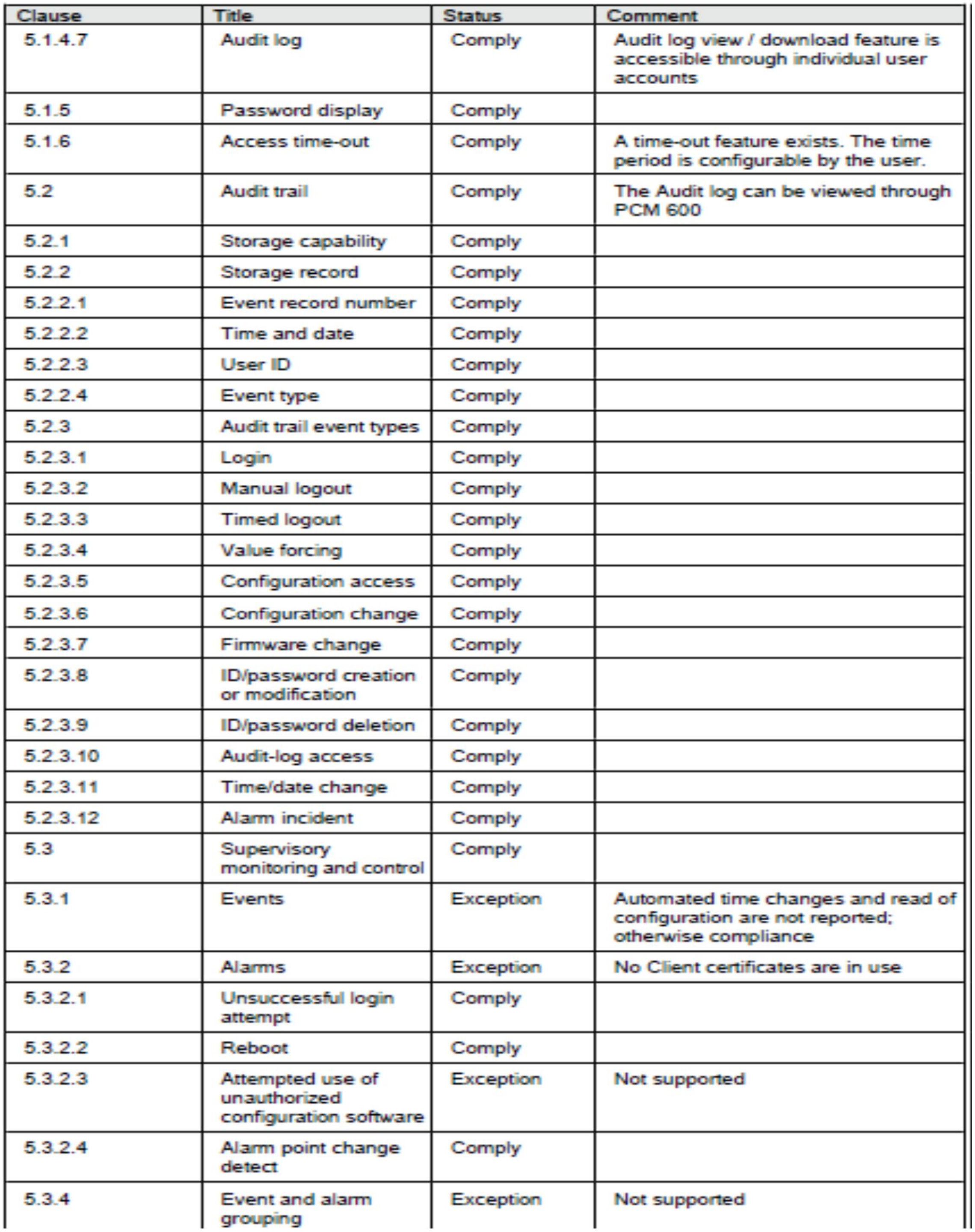
Fig 5.10 LHMI Log In Screen Shot

5.8 Compliance Statement for IED RET650 for IEEE1686:

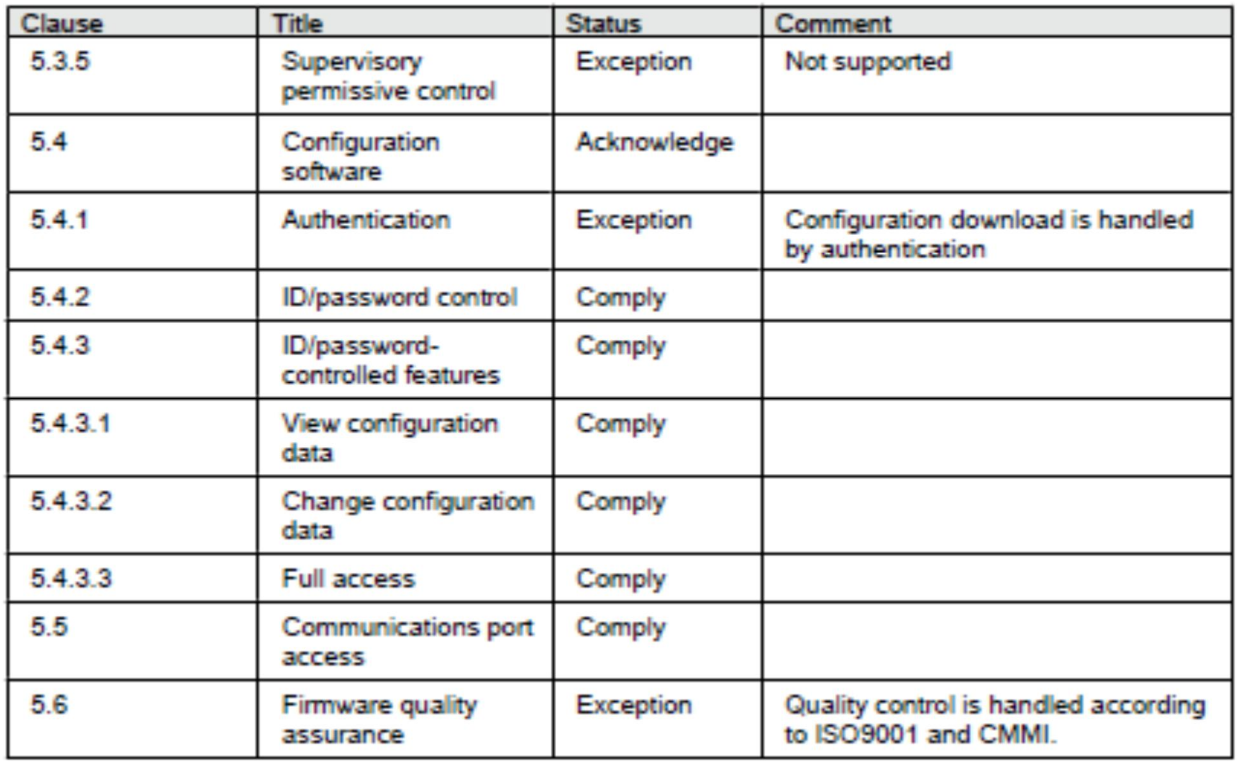
Following is the compliance statement for IED RET650 for IEEE1686 standard shown in Table 9. We can see that most of the standard requirements are met.



Clause	Title	Status	Comment
5	IED cyber security features	Acknowledge	
5.1	Electronic access control	Comply	Access is protected for local access through control panel. Access is protected for local access through a communication /diagnostic port. Access is protected for remote access through a communication media
5.1.1	Password defeat mechanisms	Comply	
5.1.2	Number of individual ID/passwords supported	Comply	20 unique ID/password combinations are supported
5.1.3	Password construction	Comply	The minimum enforced password length is configurable. If password policy is enforced, minimum is 6. Use of mix of lower and UPPERCASE characters is enforced, configurable in password policies Use of numerical values is enforced, configurable in password policies. Use of non-alphanumeric character (e.g. @, #, %, &, *) is enforced, configurable in password policies
5.1.4	Authorization levels by password	Comply	
5.1.4.1	View data	Comply	View data feature is accessible through individual user accounts
5.1.4.2	View configuration settings	Comply	View configuration settings feature is accessible through individual user accounts
5.1.4.3	Force values	Comply	Force value feature is accessible through individual user accounts
5.1.4.4	Configuration change	Comply	Configuration feature is accessible through individual user accounts
5.1.4.5	Firmware change	Comply	Firmware change feature is accessible through individual user accounts
5.1.4.6	ID/password management	Comply	User account (ID / password) management feature is accessible through individual user accounts.



Clause	Title	Status	Comment
5.1.4.7	Audit log	Comply	Audit log view / download feature is accessible through individual user accounts
5.1.5	Password display	Comply	
5.1.6	Access time-out	Comply	A time-out feature exists. The time period is configurable by the user.
5.2	Audit trail	Comply	The Audit log can be viewed through PCM 600
5.2.1	Storage capability	Comply	
5.2.2	Storage record	Comply	
5.2.2.1	Event record number	Comply	
5.2.2.2	Time and date	Comply	
5.2.2.3	User ID	Comply	
5.2.2.4	Event type	Comply	
5.2.3	Audit trail event types	Comply	
5.2.3.1	Login	Comply	
5.2.3.2	Manual logout	Comply	
5.2.3.3	Timed logout	Comply	
5.2.3.4	Value forcing	Comply	
5.2.3.5	Configuration access	Comply	
5.2.3.6	Configuration change	Comply	
5.2.3.7	Firmware change	Comply	
5.2.3.8	ID/password creation or modification	Comply	
5.2.3.9	ID/password deletion	Comply	
5.2.3.10	Audit-log access	Comply	
5.2.3.11	Time/date change	Comply	
5.2.3.12	Alarm incident	Comply	
5.3	Supervisory monitoring and control	Comply	
5.3.1	Events	Exception	Automated time changes and read of configuration are not reported; otherwise compliance
5.3.2	Alarms	Exception	No Client certificates are in use
5.3.2.1	Unsuccessful login attempt	Comply	
5.3.2.2	Reboot	Comply	
5.3.2.3	Attempted use of unauthorized configuration software	Exception	Not supported
5.3.2.4	Alarm point change detect	Comply	
5.3.4	Event and alarm grouping	Exception	Not supported



Clause	Title	Status	Comment
5.3.5	Supervisory permissive control	Exception	Not supported
5.4	Configuration software	Acknowledge	
5.4.1	Authentication	Exception	Configuration download is handled by authentication
5.4.2	ID/password control	Comply	
5.4.3	ID/password-controlled features	Comply	
5.4.3.1	View configuration data	Comply	
5.4.3.2	Change configuration data	Comply	
5.4.3.3	Full access	Comply	
5.5	Communications port access	Comply	
5.6	Firmware quality assurance	Exception	Quality control is handled according to ISO9001 and CMMI.

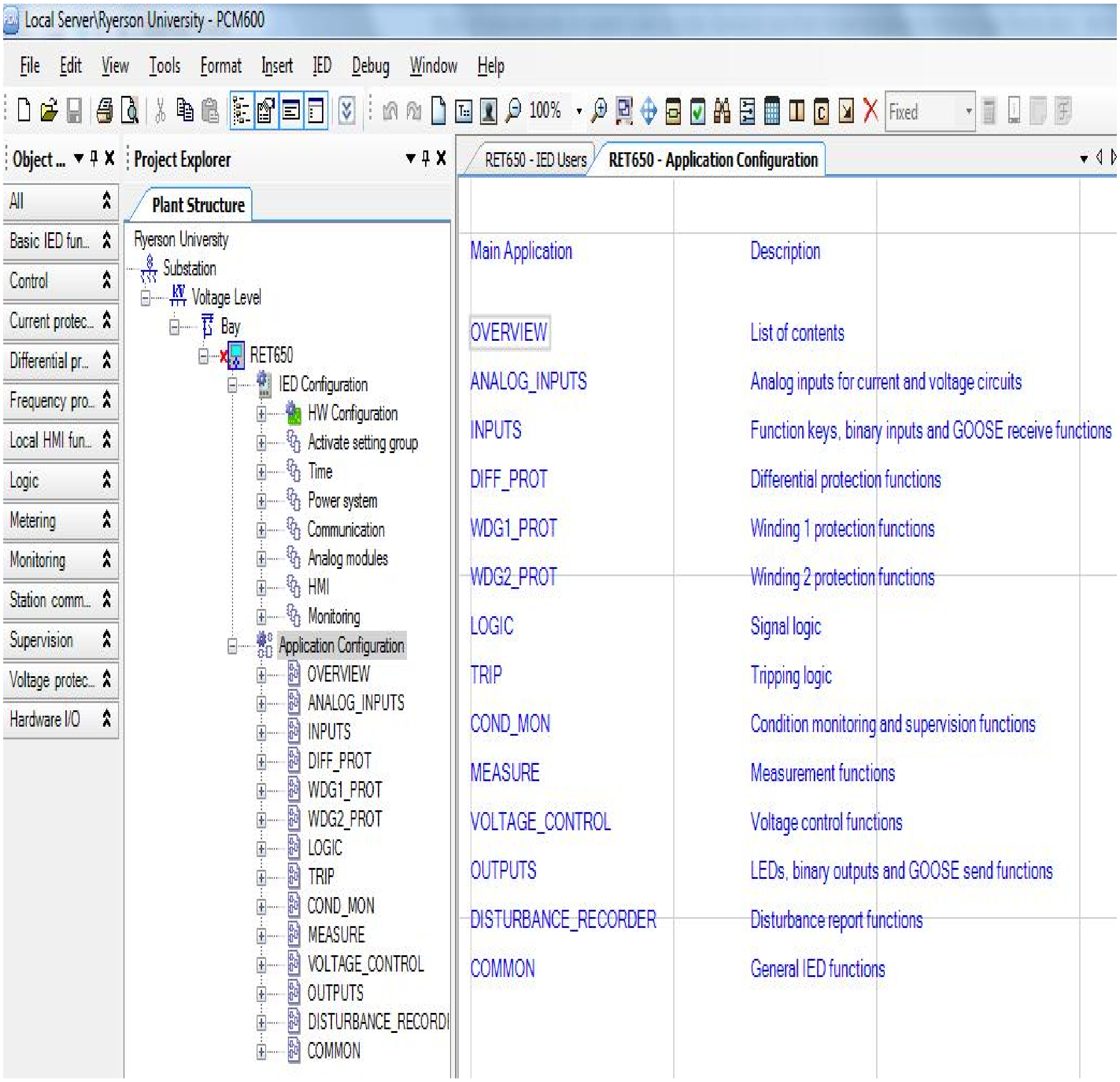
Table 9 IEEE1686 Compliance Statement for IED RET650

5.9 Application Configuration:

The IED RET650 is engineered through Application Configuration tool in PCM600. Following protection and control functionalities were implemented

Main Application	**Description**
OVERVIEW	List of Contents
ANALOG_INPUS	Analogue inputs for current and voltage circuits
INPUTS	Function Keys, binary inputs and GOOSE receive
DIFF_PROT	Differential Protection Functions
WDG1_PROT	Winding 1 protection functions
WDG2_PROT	Winding 2 protection functions
LOGIC	Signal logic
TRIP	Tripping Logic
COND_MON	Condition monitoring and supervision functions
MEASURE	Measurement functions
VOLTAGE_CONTROL	Voltage control functions
OUTPUTS	LEDs, binary outputs and GOOSE send functions
DISTURBANCE_RECORDER	Disturbance report functions
COMMON	General IED RET650 functions

A snapshot of PCM600 is shown in the following figure 5.11. The engineering drawings showing all the logic diagrams and connections to different logical nodes are attached as an APPENDIX B with this project documentation.



Main Application	Description
OVERVIEW	List of contents
ANALOG_INPUTS	Analog inputs for current and voltage circuits
INPUTS	Function keys, binary inputs and GOOSE receive functions
DIFF_PROT	Differential protection functions
WDG1_PROT	Winding 1 protection functions
WDG2_PROT	Winding 2 protection functions
LOGIC	Signal logic
TRIP	Tripping logic
COND_MON	Condition monitoring and supervision functions
MEASURE	Measurement functions
VOLTAGE_CONTROL	Voltage control functions
OUTPUTS	LEDs, binary outputs and GOOSE send functions
DISTURBANCE_RECORDER	Disturbance report functions
COMMON	General IED functions

Fig 5.11 Application Configuration for IED RET650

Chapter 6: Conclusions and Future Trends

6.1 Conclusions:

Security must be planned and designed into systems from the start. Security functions are integral to the designs of systems. Planning for security, in advance of deployment, will provide a more complete and cost effective solution. Additionally, advanced planning will ensure that security services are supportable (may be cost prohibitive to retrofit into non-planned environments. This means that security needs to be addressed at all levels of the architecture.

Security is an ever evolving process and is not static. It takes continual work and education to help the security processes keep up with the demands that will be placed on the systems. Security will continue to be a race between corporate security policies/security infrastructure and hostile entities. The security processes and systems will continue to evolve in the future. By definition there are no communication connected systems that are 100% secure. There will be always be residual risks that must be taken into account and managed. Thus, in order to maintain security, constant vigilance and monitoring are needed as well as adaptation to changes in the overall environment.

Security assessment is the process of assessing assets for their security requirements, based on probable risks of attack, liability related to successful attacks, and costs for ameliorating the risks and liabilities. The recommendations stemming from the security requirements analysis leads to the creation of security policies, the procurement of security related products and services, and the implementation of security procedures.

Security re-assessment is required periodically. The re-evaluation period needs to be prescribed for periodic review via policy. However, the policy needs to continuously evaluate the technological and political changes that may require immediate re-assessment.

Security policy generation is the process of creating policies on managing, implementing, and deploying security within a Security Domain. The recommendations produced by security assessment are reviewed, and policies are developed to ensure that the security recommendations are implemented and maintained over time.

Security deployment is a combination of purchasing and installing security products and services as well as the implementation of the security policies and procedures developed during the security policy process. As part of the deployment aspect of the Security Policies, management procedures need to be implemented that allow intrusion detection and audit capabilities, to name a few.

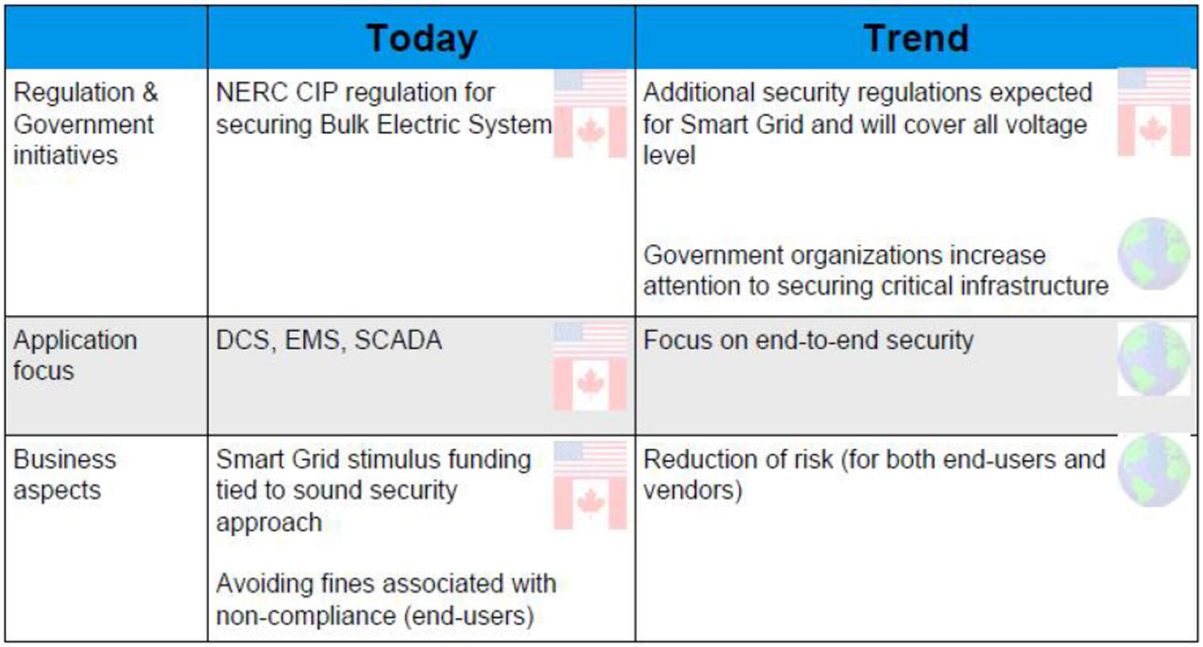
Security Training on security threats, security technologies, corporate and legal policies that impact security, Security measures analysis is a periodic, and best practices is needed. It is this training in the security process that will allow the security infrastructure to evolve.

Security audit is the process responsible for the detection of security attacks, detection of security breaches, and the performance assessment of the installed security infrastructure. However, the concept of an audit is typically applied to post event/incursion. The Security Domain model, as with active security infrastructures, requires constant monitoring. Thus the audit process needs to be enhanced.

When attempting to evaluate the security process on an enterprise basis, it is impossible to account for all of the business entities, politics, and technological choices that could be chosen by the various entities that aggregate into the enterprise. Thus to discuss security on an enterprise level is often a daunting task that may never come to closure. In order to simplify the discussion, allow for various entities to control their own resources and to enable the discussion to focus on the important aspects.

6.2 FUTURE TRENDS

As our control systems are becoming more and more complex with the modernization in power sector. Now there is an ever increasing need for the network security of power systems and how they communicate with each other on network level. As interaction between different components of power systems is inevitable, thus there is a huge potential in this area. The following table no. 10 describes today and future trends.



	Today	Trend
Regulation & Government initiatives	NERC CIP regulation for securing Bulk Electric System 🇺🇸🇨🇦	Additional security regulations expected for Smart Grid and will cover all voltage level 🇺🇸🇨🇦 Government organizations increase attention to securing critical infrastructure 🌍
Application focus	DCS, EMS, SCADA 🇺🇸🇨🇦	Focus on end-to-end security 🌍
Business aspects	Smart Grid stimulus funding tied to sound security approach 🇺🇸🇨🇦 Avoiding fines associated with non-compliance (end-users)	Reduction of risk (for both end-users and vendors) 🌍

Table 10 Future Trends

Appendix A: Excerpts of IEC62351 & IEEE1686

TECHNICAL SPECIFICATION

IEC TS 62351-6

First edition
2007-06

Power systems management and associated information exchange – Data and communications security –

Part 6: Security for IEC 61850

Reference number
IEC/TS 62351-6:2007(E)

IEC Central Office
3, rue de Varembé
CH-1211 Geneva 20
Switzerland
Email: inmail@iec.ch
Web: www.iec.ch

TECHNICAL SPECIFICATION

IEC TS 62351-6

First edition
2007-06

Power systems management and associated information exchange – Data and communications security –

Part 6: Security for IEC 61850

Commission Electrotechnique Internationale
International Electrotechnical Commission
Международная Электротехническая Комиссия

PRICE CODE P

For price, see current catalogue

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

POWER SYSTEMS MANAGEMENT AND ASSOCIATED INFORMATION EXCHANGE – DATA AND COMMUNICATIONS SECURITY –

Part 6: Security for IEC 61850

FOREWORD

1) The International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of IEC is to promote international co-operation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, IEC publishes International Standards, Technical Specifications, Technical Reports, Publicly Available Specifications (PAS) and Guides (hereafter referred to as “IEC Publication(s)”). Their preparation is entrusted to technical committees; any IEC National Committee interested in the subject dealt with may participate in this preparatory work. International, governmental and non-governmental organizations liaising with the IEC also participate in this preparation. IEC collaborates closely with the International Organization for Standardization (ISO) in accordance with conditions determined by agreement between the two organizations.
2) The formal decisions or agreements of IEC on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC National Committees.
3) IEC Publications have the form of recommendations for international use and are accepted by IEC National Committees in that sense. While all reasonable efforts are made to ensure that the technical content of IEC Publications is accurate, IEC cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.
4) In order to promote international uniformity, IEC National Committees undertake to apply IEC Publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC Publication and the corresponding national or regional publication shall be clearly indicated in the latter.
5) IEC provides no marking procedure to indicate its approval and cannot be rendered responsible for any equipment declared to be in conformity with an IEC Publication.
6) All users should ensure that they have the latest edition of this publication.
7) No liability shall attach to IEC or its directors, employees, servants or agents including individual experts and members of its technical committees and IEC National Committees for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this IEC Publication or any other IEC Publications.
8) Attention is drawn to the Normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.
9) Attention is drawn to the possibility that some of the elements of this IEC Publication may be the subject of patent rights. IEC shall not be held responsible for identifying any or all such patent rights.

The main task of IEC technical committees is to prepare International Standards. In exceptional circumstances, a technical committee may propose the publication of a technical specification when

- the required support cannot be obtained for the publication of an International Standard, despite repeated efforts, or
- the subject is still under technical development or where, for any other reason, there is the future but no immediate possibility of an agreement on an International Standard.

Technical specifications are subject to review within three years of publication to decide whether they can be transformed into International Standards.

IEC 62351-6, which is a technical specification, has been prepared by IEC technical committee 57: Power systems management and associated information exchange.

The text of this technical specification is based on the following documents:

Enquiry draft	Report on voting
57/805/DTS	57/859/RVC

Full information on the voting for the approval of this technical specification can be found in the report on voting indicated in the above table.

This publication has been drafted in accordance with the ISO/IEC Directives, Part 2.

A list of all parts of the IEC 62351 series, published under the general title *Power systems management and associated information exchange – Data and communications security,* can be found on the IEC website.

The committee has decided that the contents of this publication will remain unchanged until the maintenance result date indicated on the IEC web site under "http://webstore.iec.ch" in the data related to the specific publication. At this date, the publication will be

- transformed into an International standard,
- reconfirmed,
- withdrawn,
- replaced by a revised edition, or
- amended.

A bilingual version of this publication may be issued at a later date.

POWER SYSTEMS MANAGEMENT AND ASSOCIATED INFORMATION EXCHANGE – DATA AND COMMUNICATIONS SECURITY –

Part 6: Security for IEC 61850

1 Scope and object

1.1 Scope

This part of IEC 62351 specifies messages, procedures, and algorithms for securing the operation of all protocols based on or derived from the standard IEC 61850. This specification applies to at least those protocols listed in Table 1.

Table 1 – Scope of application to standards

Number	Name
IEC 61850-8-1	Communication networks and systems in substations – Part 8-1: Specific Communication Service Mapping (SCSM) – Mappings to MMS (ISO/IEC 9506-1 and ISO/IEC 9506-2) and to ISO/IEC 8802-3
IEC 61850-9-2	Communication networks and systems in substations – Part 9-2: Specific Communication Service Mapping (SCSM) – Sampled values over ISO/IEC 8802-3
IEC 61850-6	Communication networks and systems in substations – Part 6: Configuration description language for communication in electrical substations related to IEDs

1.2 Object

The initial audience for this specification is intended to be the members of the working groups developing or making use of the protocols listed in Table 1. For the measures described in this specification to take effect, they must be accepted and referenced by the specifications for the protocols themselves. This document is written to enable that process.

The subsequent audience for this specification is intended to be the developers of products that implement these protocols.

Portions of this specification may also be of use to managers and executives in order to understand the purpose and requirements of the work.

2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

IEC 61850 (all parts), *Communication networks and systems in substations*

IEC 61850-6, *Communication networks and systems in substations – Part 6: Configuration description language for communication in electrical substations related to IEDs*

IEC 61850-8-1, *Communication networks and systems in substations – Part 8-1: Specific Communication Service Mapping (SCSM) – Mappings to MMS (ISO 9506-1 and ISO 9506-2) and to ISO/IEC 8802-3*

IEC 61850-9-1, *Communication networks and systems in substations – Part 9-1: Specific Communication Service Mapping (SCSM) – Sampled values over serial unidirectional multidrop point to point link*

IEC 61850-9-2, *Communication networks and systems in substations – Part 9-2: Specific Communication Service Mapping (SCSM) – Sampled values over ISO/IEC 8802-3*

IEC 62351-1, *Power systems management and associated information exchange – Data and communications security – Part 1: Communication network and system security – Introduction to security issues*

IEC 62351-2, *Power systems management and associated information exchange – Data and communications security – Part 2: Glossary of terms*

IEC 62351-4, *Power systems management and associated information exchange – Data and communications security – Part 4: Profiles including MMS*

ISO 9506 (all parts), *Industrial automation systems – Manufacturing Message Specification*

ISO/IEC 8802-3, *Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements – Part 3: Carrier sense multiple access with collision detection (CSMA/CD) access method and physical layer specifications*

ISO/IEC 13239, *Information technology – Telecommunications and information exchange between systems – High-level data link control (HDLC) procedures*

IEEE Std. 802.1Q-2003, *Virtual Bridged Local Area Networks*

RFC 2030, *Simple Network Time Protocol (SNTP) Version 4 for IPv4, IPv6 and OSI*

RFC 2313, *PKCS #1: RSA Encryption Version 1.5*

RFC 3447, *Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1*

RFC 4634, *US Secure Hash Algorithms (SHA and HMAC-SHA)*

3 Definitions

For the purposes of this document, the terms and definitions contained in IEC 62351-2 apply.

4 Security issues addressed by this specification

4.1 Operational issues affecting choice of security options

For applications using GOOSE and IEC 61850-9-2 and requiring 4 ms response times, multicast configurations and low CPU overhead, encryption is not recommended. Instead, the communication path selection process (e.g. the fact that GOOSE and SMV are supposed to be restricted to a logical substation LAN) shall be used to provide confidentiality for information exchanges. However, this specification does define a mechanism for allowing confidentiality for applications where the 4 ms delivery criterion is not a concern.

NOTE The actual performance characteristics of an implementation claiming conformance to this technical specification is outside the scope of this specification.

With the exception of confidentiality, this specification sets forth a mechanism that allows co-existence of secure and non-secure PDUs.

4.2 Security threats countered

See IEC 62351-1 for a discussion of security threats and attack methods.

If encryption is not employed, then the specific threats countered in this part include:

- unauthorized modification of information through message level authentication of the messages.

If encryption is employed, then the specific threats countered in this part include:

- unauthorized access to information through message level authentication and encryption of the messages;
- unauthorized modification (tampering) or theft of information through message level authentication and encryption of the messages.

4.3 Attack methods countered

The following security attack methods are intended to be countered through the appropriate implementation of the specification/recommendations found within this document:

- man-in-the-middle: this threat will be countered through the use of a Message Authentication Code mechanism specified within this document;
- tamper detection/message integrity: These threats will be countered through the algorithm used to create the authentication mechanism as specified within this document;
- replay: this threat will be countered through the use of specialized processing state machines specified within IEC 62351-4 and this document.

5 Correlation of IEC 61850 parts and IEC 62351 parts

5.1 IEC 61850 security for profiles using ISO 9506 (MMS)

5.1.1 General

IEC 61850 implementations claiming conformance to this specification and declaring support for the IEC 61850-8-1 profile utilizing TCP/IP and ISO 9506 (MMS) shall implement Clauses 5 and 6 of IEC 62351-4. In addition to the IEC 62351-4 specification, extensions to IEC 61850-6 (the Substation Configuration Language) shall be supported as prescribed in 7.2.3.

IEC 61850-8-1 specifies the use of MMS within a substation. However, the scope of this specification provides security specifications for use within the substation and external to the substation (e.g. Control Centre to Substation).

5.1.2 Control centre to substation

The IEC 62351-4 standard shall be used without any other additions.

5.1.3 Substation communications

The following cipher suite shall be supported in addition to those specified in IEC 62351-4.

TLS_DH_RSA_WITH_AES_128_SHA

NOTE This additional cipher suite is suggested in order to allow less CPU utilization when the communication environment is within a substation.

5.2 IEC 61850 security for profiles using VLAN IDs

For the IEC 61850 profiles specified that make use of VLAN IDs (e.g. IEC 61850-8-1 GOOSE, IEC 61850-9-1, and IEC 61850-9-2) profile security shall be provided as specified in Clause 7.

6 IEC 61850 security for SNTP

RFC 2030, including mandatory use of the authentication algorithms, shall be used.

7 IEC 61850 security for profiles using VLAN technologies

7.1 Overview of VLAN usage and IEC 61850 (informative)

This specification extends the normal IEC 61850 GOOSE and SMV PDUs. The outline of a PDU for GSE Management and GOOSE is given in Annex C of IEC 61850-8-1.

7.2 Extended PDU

7.2.1 General format of extended PDU

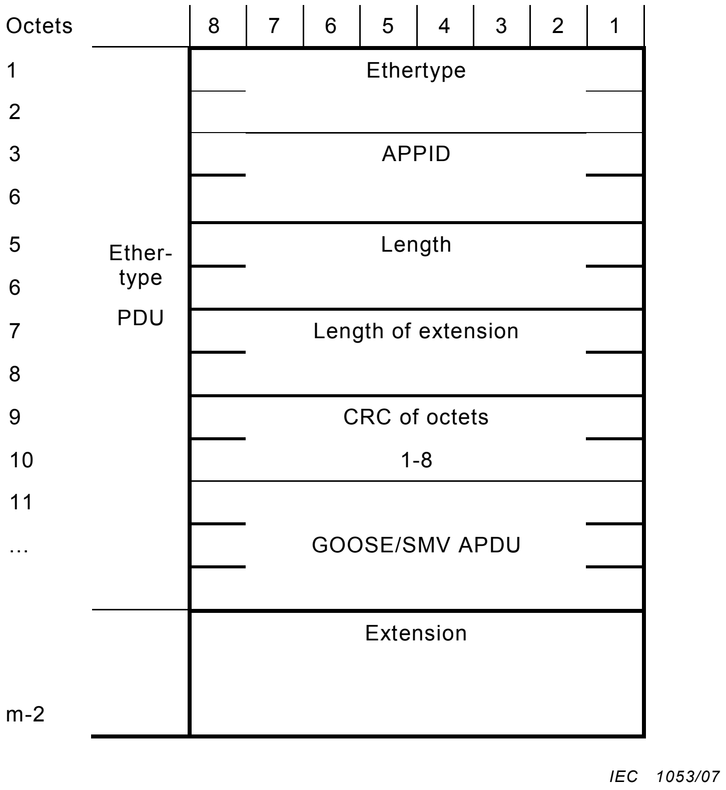


Figure 1 – General format of extended PDU

Figure 1 depicts the fact that the Reserved1 and Reserved2 fields are to be used for implementations claiming conformance to this specification in regards to GOOSE and SMV. This specification specifies that the:

- **Reserved1 field** shall be used to specify the number of octets conveyed by the extension octets. This value shall be contained in the first octet of the Reserved1 field. The valid range of values is zero(0) through 255. A value of zero(0) shall indicate that no extension octets are present.

  The second octet of the Reserved1 field shall be reserved for future use;

- **Reserved2** field shall contain a 16-bit CRC, as calculated per ISO/IEC 13239 (ISO HDLC). The CRC shall be calculated over Octets 1-8 of the VLAN information of the Extended PDU.

  The CRC shall be present if the Extension Length has a non-zero value.

7.2.2 Format of extension octets

The format of the extension octet area shall be:

```
Extension::= {
   [0] IMPLICIT SEQUENCE {
        [1] IMPLICIT SEQUENCE Reserved OPTIONAL,
        [2] IMPLICIT OCTETSTRING Private  OPTIONAL,
        [3] IMPLICIT AuthenticationValue OPTIONAL,
        …
                    }
}
```

Extension shall be encoded per ASN.1 Basic Encoding Rules.

The Reserved SEQUENCE is used to reserve future standardized extension per this specification. If no extension, besides Authentication and Encryption is defined in this specification, this SEQUENCE shall not be present.

Therefore a SEQUENCE of NULL length shall be considered non-conformant to this specification.

The Private SEQUENCE is provided to allow vendors to convey Private information. The scope of the semantics and syntax of the contents of this SEQUENCE is out-of-scope of this specification and shall only be interoperable via prior agreement. This SEQUENCE shall only be present if there are actual contents being conveyed.

7.2.2.1 &AuthenticationValue Algorithm

The algorithm for AuthenticationValue generation is based upon the generation of a reproducible Message Authentication Code (MAC).

The MAC shall be generated through the computation of a SHA256 hash per RFC 4634. The hash shall contain all octets of the Extended PDU with the exception of the Tag, Length, Value of the

AuthenticationValue.

The value of the hash shall then be digitally signed.

The definition for digital signature is found in RFC 2313:

> "For digital signatures, the content to be signed is first reduced to a message digest with a message-digest algorithm (such as MD5), and then an octet string containing the message digest is encrypted with the RSA private key of the signer of the content. The content and the encrypted message digest are represented together according to the syntax in PKCS #7 to yield a digital signature."

NOTE The reference to MD5, in the definition, is not normative. It is an example given in the RFC 2313 quoted text.

RFC 3447 (specification for PKCS#1 Version 2.1) specifies RSASA-PSS. This is the algorithm that shall be used by implementations claiming conformance to this specification. The use of RFC 3447 shall be restricted to those abilities/capabilities that are compatible with PKCS Version 1.5 (RFC 2313). The Hash algorithm shall be SHA256

The value of the AuthenticationValue shall be encoded as an ASN.1 OCTETSTRING.

7.2.2.2 Requirements on servers

Servers shall perform the algorithm as previously specified. If the server is not providing the AuthenticationValue, the AuthenticationValue shall not be present in the Extension octets.

Additionally, implementations that use the AuthenticationValue shall provide a public X,509 certificate for installation on the receiving clients.

7.2.2.3 Requirements on clients

The subscribing client must have a local means of referencing the Source MAC Address to the AES 128 bit public Key provided by the server.

NOTE It is recommended that the actual certificate be stored for this purpose, although it is not a requirement.

If there is no reference, then security extensions/processing should not occur.

Upon receiving a VLAN tagged GOOSE or SMV message, where security extension are configured:

- the receiving client shall calculate the AuthenticationValue for the APDU as specified in clause 7.2.2.1;
- the Reserved octets shall be decrypted by using the appropriate key and algorithm (reverse of clause 7.2.2.1);
- if the calculated AuthenticationValue and de-signed AuthenticationValue match, then the client should proceed with the processing of the APDU.

7.2.2.4 GOOSE replay

In order to augment and protect from GOOSE replay, the security extensions shall be used. Additionally, the following should be used.

- The process of verifying the AuthenticationValue (see 7.2.2.3) shall occur prior to the additional processing within this clause.
- The client should establish and track its current time. A GOOSE whose timestamp exceeds a 2 min skew should not be processed. The skew period shall be configurable and it shall support a maximum-minimum of 10 s.
- The client should apply skew filtering for Stnum changes only.
- The client should record and track the received Stnum for the publishing server. If a lesser value for Stnum is received, and there has been no rollover or timeallowedtoLive timeout, the message should be discarded.
- If there is a message timeout, the starting Stnum shall be re-established.
- If Stnum rolls-over, the starting Stnum shall be re-established.
- Upon initialisation/power-up the starting Stnum shall be zero (0).

7.2.2.5 SMV replay

7.2.2.5.1 Server processing

In order to prevent SMV replay, the Security field of the SMV protocol shall be utilized (see Table 2).

Table 2 – Extract from IEC 61850-9-2 (informative)

ASN.1 Basic Encoding Rules (BER) **SavPdu::=** SEQUENCE {
noASDU [0] IMPLICIT INTEGER (1..65535),
security [1] ANY OPTIONAL,
asdu [2] IMPLICIT SEQUENCE OF ASDU **}**

Prevention of replay requires that the MAC security extensions shall be used in order to prevent tampering and that the security field be specified as follows:

```
IMPORT

security::=  [0] IMPLICIT SEQUENCE {
                    timestamp [0] IMPLICIT UTCtime, --time of send
                   }
```

&timestamp

The timestamp attribute shall represent the approximate time at which the SMV frame was formatted.

7.2.2.5.2 Client processing

Based upon the SMV security field being present, the following client rules shall apply:

- The client should establish track its current time. A SMV whose timestamp exceeds a 2 min skew should not be processed.
- The client should record and track the received smpCnt for the publishing server. If a lesser value for sqNum is received, and there has been no rollover the message should be discarded.
- If there is a message timeout, the starting Stnum shall be re-established.
- If sqNum rolls-over, the starting sqNum shall be re-established.

Upon initialisation/power-up the starting sqNum shall be zero (0).

7.2.3 Substation configuration language

7.2.3.1 SCL certificate extension

7.2.3.1.1 SCL certificate extension structure

Additionally, the SCL shall be extended to include the following to allow definition of certificates that are to be used.

```
<xs:complexType name="tCertificate">
        <xs:complexContent>
            <xs:extension base="tNaming">
            <xs:sequence>
                    <xs:element name="XferNumber" type="xs:unsignedInt" minOccurs="0"
maxOccurs="1"  />
                    <xs:element name="SerialNumber" type="xs:normalizedString" minOccurs="1"
maxOccurs="1"  />
                    <xs:element name="Subject" type="tcert" minOccurs="1" maxOccurs="1"/>
                    <xs:element name="IssuerName" type="tcert" minOccurs="1" maxOccurs="1"/>
            </xs:sequence>
        </xs:complexContent>
</xs:complexType>

<xs:complexType name="tcert">
        <xs:complexContent>
            <xs:extension base="tNaming">
            <xs:sequence>
                    <xs:element name="CommonName" type="xs:normalizedString" minOccurs="1"
maxOccurs="1" >
                    <xs:element name="IDHeirarchy" type="xs:normalizedString" minOccurs="1"  />
            </xs:sequence>
        </xs:complexContent>
</xs:complexType>
```

IEC 1054/07

Figure 2 – SCL extensions for certificates

7.2.3.1.2 &XferNumber

This attribute shall be used to convey the number through which the sending IED shall refer to the certificate. The attribute value shall be present if the certificate is to be used for GOOSE or SMV. The valid range of values is 0 through 7.

7.2.3.1.3 &SerialNumber

This attribute shall contain the serial number value of the certificate.

7.2.3.1.4 &Subject

This complex type shall contain the identifying hierarchy of the certificate as present within the certificate for the Subject in the certificate.

7.2.3.1.5 &IssuerName

This complex type shall contain the identifying hierarchy of the certificate as present within the certificate for the IssuerName in the certificate.

7.2.3.1.6 &CommonName

This attribute shall contain the value of the CommonName as found within the certificate.

7.2.3.2 Specification of AccessPoint security usage

```
<xs:complexType name="tAccessPoint">
    <xs:complexContent>
        <xs:extension base="tNaming">
            <xs:choice minOccurs="0">
                <xs:element name="Server" type="tServer">
                    <xs:unique name="uniqueAssociationInServer">
                        <xs:selector xpath="./scl:Association"/>
                        <xs:field xpath="@associationID"/>
                    </xs:unique>
                </xs:element>
                <xs:element ref="LN" maxOccurs="unbounded"/>
            </xs:choice>
            <xs:attribute name="router" type="xs:boolean" use="optional" default="false">
            </xs:attribute>
            <xs:attribute name="clock" type="xs:boolean" use="optional" default="false">
            </xs:attribute>
            <xs:element name="GOOSESecurity" type="tCertificate" use="optional" maxOccurs="7" >
            <xs:element name="SMVSecurity" type="tCertificate" use="optional" maxOccurs="7" >
        </xs:extension>
    </xs:complexContent>
</xs:complexType>
```

IEC 1055/07

Figure 3 – Extension to AccessPoint SCL definition

The AccessPoint SCL definition shall be extended to include GOOSESecurity and SMVSecurity for implementations claiming conformance to this specification a support for the appropriate security (e.g. GOOSE or SMV).

Implementations claiming to support Secure GOOSE shall have a minimum of one GOOSESecurity element present.

Implementations claiming to support Secure SMV shall have a minimum of one SMVSecurity element present.

Implementations claiming to support encryption, shall include the GOOSEEncryptioninUse or SMVEncryptioninUse attribute whose value(s) shall be the same as the XferNumber for the certificate intended to be used for both authentication and encryption.

8 Conformance

8.1 General conformance

Implementations claiming conformance to this specification shall provide an extended Protocol Implementation Conformance Statement (PICS) as set forth in the following clauses. For some profiles, additional Protocol Implementation eXtra InformaTion (PIXIT) information may need to be provided.

For the following clauses and tables, the following definitions apply:

- m: mandatory support – the item shall be implemented;
- c: conditional support – the item shall be implemented if the stated condition exists;
- o: optional support – the implementation may decide to implement the item;
- x: excluded – the implementation shall not implement this item;
- i: out-of-scope – the implementation of the item is not within the scope of this specification.

The information in Table 3 shall be provided for an implementation claiming support for this specification.

Table 3 – Conformance table

		Client		Server		Value/Comment
		f/s		f/s		
G1	Support for IEC 61850-8-1/ISO 9506 security	o	C1	o	C1	
G2	Support for IEC 61850-8-1 GOOSE security	o	C1	o	C1	
G3	Support for IEC 61850-9-2 SMV security	o	C1	o	C1	
G4	Support for SNTP security	o		o		
C1 – At least one shall have support declared.						

8.2 Conformance for implementations claiming ISO 9506 profile security

The information in Table 4 shall be provided for implementations claiming support of the security profile for ISO 9506 / IEC 61850 profile.

Table 4 – PICS for ISO 9506 profile

		Client		Server		Value/Comment
		f/s		f/s		
S1	ACSE Authentication	m		m		
S2	IEC 62351-4 Support	m		m		
S3A	Mandatory Cipher Suite	m		m		
S3B	TLS_DH_RSA_WITH_AES_128_SHA	o		m		

8.3 Conformance for implementations claiming VLAN profile security

The information in Table 5 shall be provided for implementations claiming support of the security profile for VLAN IEC 61850 profile.

Table 5 – PICS for VLAN profiles

		Client		Server		Value/Comment
		f/s		f/s		
S4	SCL extensions	m		m		
S4a	IEC 61850-8-1 GOOSE security	C1		C1		
S4b	IEC 61850-9-2 SMV security	C2		C2		
C1 – shall be “m” for implementations claiming GOOSE security conformance. C2 – shall be “m” for implementation claiming SMV security conformance.						

8.4 Conformance for implementations claiming SNTP profile security

The information shall be provided for implementations claiming support of the security profile for SNTP IEC 61850 profile.

Table 6 – PICS for SNTP profiles

		Client		**Server**		**Value/Comment**
		f/s		f/s		
S7	RFC 2030	m		m		

Bibliography

IEC 62351-3, *Power systems management and associated information exchange – Data and communications security – Part 3: Communication network and system security – Profiles including TCP/IP*

RFC 2104, *HMAC: Keyed-Hashing for Message Authentication*

RFC 2437, *PKCS #1: RSA Cryptography Specifications Version 2.0*

RFC 3174, *Secure Hash Algorithm (SHA1)*

ICS 33.200

ISBN 2-8318-9188-4

9 782831 891880

Typeset and printed by the IEC Central Office
GENEVA, SWITZERLAND

IEEE STANDARDS ASSOCIATION

IEEE Standard for Intelligent Electronic Devices Cyber Security Capabilities

IEEE Power and Energy Society

Sponsored by the
Substations Committee
and the
Transmission and Distribution Committee

IEEE
3 Park Avenue
New York, NY 10016-5997
USA

IEEE Std 1686™-2013
(Revision of
IEEE Std 1686-2007)

IEEE Std 1686™-2013
(Revision of
IEEE Std 1686-2007)

IEEE Standard for Intelligent Electronic Devices Cyber Security Capabilities

Sponsor

Substations Committee
and the
Transmission and Distribution Committee
of the
IEEE Power and Energy Society

Approved 11 December 2013

IEEE-SA Standards Board

Abstract: The functions and features to be provided in intelligent electronic devices (IEDs) to accommodate critical infrastructure protection programs are defined in this standard. Security regarding the access, operation, configuration, firmware revision and data retrieval from an IED are addressed. Communications for the purpose of power system protection (teleprotection) are not addressed in this standard.

Keywords: CIP, critical infrastructure protection, cyber, IED, IEEE 1686™, intelligent electronic device, security, substation.

The Institute of Electrical and Electronics Engineers, Inc.
3 Park Avenue, New York, NY 10016-5997, USA

PDF: ISBN 978-0-7381-8824-9 STD98482
Print: ISBN 978-0-7381-8825-6 STDPD98482

Important Notices and Disclaimers Concerning IEEE Standards Documents

IEEE documents are made available for use subject to important notices and legal disclaimers. These notices and disclaimers, or a reference to this page, appear in all standards and may be found under the heading "Important Notice" or "Important Notices and Disclaimers Concerning IEEE Standards Documents."

Notice and Disclaimer of Liability Concerning the Use of IEEE Standards Documents

IEEE Standards documents (standards, recommended practices, and guides), both full-use and trial-use, are developed within IEEE Societies and the Standards Coordinating Committees of the IEEE Standards Association ("IEEE-SA") Standards Board. IEEE ("the Institute") develops its standards through a consensus development process, approved by the American National Standards Institute ("ANSI"), which brings together volunteers representing varied viewpoints and interests to achieve the final product. Volunteers are not necessarily members of the Institute and participate without compensation from IEEE. While IEEE administers the process and establishes rules to promote fairness in the consensus development process, IEEE does not independently evaluate, test, or verify the accuracy of any of the information or the soundness of any judgments contained in its standards.

IEEE does not warrant or represent the accuracy or content of the material contained in its standards, and expressly disclaims all warranties (express, implied and statutory) not included in this or any other document relating to the standard, including, but not limited to, the warranties of: merchantability; fitness for a particular purpose; non-infringement; and quality, accuracy, effectiveness, currency, or completeness of material. In addition, IEEE disclaims any and all conditions relating to: results; and workmanlike effort. IEEE standards documents are supplied "AS IS" and "WITH ALL FAULTS."

Use of an IEEE standard is wholly voluntary. The existence of an IEEE standard does not imply that there are no other ways to produce, test, measure, purchase, market, or provide other goods and services related to the scope of the IEEE standard. Furthermore, the viewpoint expressed at the time a standard is approved and issued is subject to change brought about through developments in the state of the art and comments received from users of the standard.

In publishing and making its standards available, IEEE is not suggesting or rendering professional or other services for, or on behalf of, any person or entity nor is IEEE undertaking to perform any duty owed by any other person or entity to another. Any person utilizing any IEEE Standards document, should rely upon his or her own independent judgment in the exercise of reasonable care in any given circumstances or, as appropriate, seek the advice of a competent professional in determining the appropriateness of a given IEEE standard.

IN NO EVENT SHALL IEEE BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO: PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE PUBLICATION, USE OF, OR RELIANCE UPON ANY STANDARD, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE AND REGARDLESS OF WHETHER SUCH DAMAGE WAS FORESEEABLE.

Translations

The IEEE consensus development process involves the review of documents in English only. In the event that an IEEE standard is translated, only the English version published by IEEE should be considered the approved IEEE standard.

Official statements

A statement, written or oral, that is not processed in accordance with the IEEE-SA Standards Board Operations Manual shall not be considered or inferred to be the official position of IEEE or any of its committees and shall not be considered to be, or be relied upon as, a formal position of IEEE. At lectures, symposia, seminars, or educational courses, an individual presenting information on IEEE standards shall make it clear that his or her views should be considered the personal views of that individual rather than the formal position of IEEE.

Comments on standards

Comments for revision of IEEE Standards documents are welcome from any interested party, regardless of membership affiliation with IEEE. However, IEEE does not provide consulting information or advice pertaining to IEEE Standards documents. Suggestions for changes in documents should be in the form of a proposed change of text, together with appropriate supporting comments. Since IEEE standards represent a consensus of concerned interests, it is important that any responses to comments and questions also receive the concurrence of a balance of interests. For this reason, IEEE and the members of its societies and Standards Coordinating Committees are not able to provide an instant response to comments or questions except in those cases where the matter has previously been addressed. For the same reason, IEEE does not respond to interpretation requests. Any person who would like to participate in revisions to an IEEE standard is welcome to join the relevant IEEE working group.

Comments on standards should be submitted to the following address:

Secretary, IEEE-SA Standards Board
445 Hoes Lane
Piscataway, NJ 08854 USA

Laws and regulations

Users of IEEE Standards documents should consult all applicable laws and regulations. Compliance with the provisions of any IEEE Standards document does not imply compliance to any applicable regulatory requirements. Implementers of the standard are responsible for observing or referring to the applicable regulatory requirements. IEEE does not, by the publication of its standards, intend to urge action that is not in compliance with applicable laws, and these documents may not be construed as doing so.

Copyrights

IEEE draft and approved standards are copyrighted by IEEE under U.S. and international copyright laws. They are made available by IEEE and are adopted for a wide variety of both public and private uses. These include both use, by reference, in laws and regulations, and use in private self-regulation, standardization, and the promotion of engineering practices and methods. By making these documents available for use and adoption by public authorities and private users, IEEE does not waive any rights in copyright to the documents.

Photocopies

Subject to payment of the appropriate fee, IEEE will grant users a limited, non-exclusive license to photocopy portions of any individual standard for company or organizational internal use or individual, non-commercial use only. To arrange for payment of licensing fees, please contact Copyright Clearance Center, Customer Service, 222 Rosewood Drive, Danvers, MA 01923 USA; +1 978 750 8400. Permission to photocopy portions of any individual standard for educational classroom use can also be obtained through the Copyright Clearance Center.

Updating of IEEE Standards documents

Users of IEEE Standards documents should be aware that these documents may be superseded at any time by the issuance of new editions or may be amended from time to time through the issuance of amendments, corrigenda, or errata. An official IEEE document at any point in time consists of the current edition of the document together with any amendments, corrigenda, or errata then in effect.

Every IEEE standard is subjected to review at least every ten years. When a document is more than ten years old and has not undergone a revision process, it is reasonable to conclude that its contents, although still of some value, do not wholly reflect the present state of the art. Users are cautioned to check to determine that they have the latest edition of any IEEE standard.

In order to determine whether a given document is the current edition and whether it has been amended through the issuance of amendments, corrigenda, or errata, visit the IEEE-SA Website at http://ieeexplore.ieee.org/xpl/standards.jsp or contact IEEE at the address listed previously. For more information about the IEEE–SA or IEEE's standards development process, visit the IEEE-SA Website at http://standards.ieee.org.

Errata

Errata, if any, for all IEEE standards can be accessed on the IEEE-SA Website at the following URL: http://standards.ieee.org/findstds/errata/index.html. Users are encouraged to check this URL for errata periodically.

Patents

Attention is called to the possibility that implementation of this standard may require use of subject matter covered by patent rights. By publication of this standard, no position is taken by the IEEE with respect to the existence or validity of any patent rights in connection therewith. If a patent holder or patent applicant has filed a statement of assurance via an Accepted Letter of Assurance, then the statement is listed on the IEEE-SA Website at http://standards.ieee.org/about/sasb/patcom/patents.html. Letters of Assurance may indicate whether the Submitter is willing or unwilling to grant licenses under patent rights without compensation or under reasonable rates, with reasonable terms and conditions that are demonstrably free of any unfair discrimination to applicants desiring to obtain such licenses.

Essential Patent Claims may exist for which a Letter of Assurance has not been received. The IEEE is not responsible for identifying Essential Patent Claims for which a license may be required, for conducting inquiries into the legal validity or scope of Patents Claims, or determining whether any licensing terms or conditions provided in connection with submission of a Letter of Assurance, if any, or in any licensing agreements are reasonable or non-discriminatory. Users of this standard are expressly advised that determination of the validity of any patent rights, and the risk of infringement of such rights, is entirely their own responsibility. Further information may be obtained from the IEEE Standards Association.

Participants

At the time this IEEE standard was completed, the Application of Computer-Based Systems Working Group had the following membership:

Samuel Sciacca, *Chair*
Marc LaCroix, *Vice Chair*

Ed Cenzon
Mason Clark
Michael Dood
Didier Giarratano
Robert Haberman
Chris Huntley
Rick Liposchak
Greg Luri
Harsh Naik
Craig Preuss
John Tengdin
Eric Thibodeau
Stephen Thompson
Tim Tibbals

The following members of the individual balloting committee voted on this standard. Balloters may have voted for approval, disapproval, or abstention.

William Ackerman
Ali Al Awazi
Steven Alexanderson
John Banting
Philip Beaumont
Oscar Bolado
James Bougie
Chris Brooks
Bill Brown
Gustavo Brunello
Paul Cardinal
James Cornelison
Michael Dood
Ernest Duckworth
Sourav Dutta
Kenneth Fodero
Fredric Friend
Frank Gerleve
Mietek Glinkowski
Roman Graf
Randall Groves
John Harauz
Roger Hedding
David Herrell
Gary Heuston
Werner Hoelzl
Gary Hoffman
Dennis Holstein
Noriyuki Ikeuchi
R. Jackson
Brian Johnson
Gerald Johnson
Piotr Karocki
Yuri Khersonsky
Stanley Klein
Jim Kulchisky
Marc LaCroix
Chung-Yiu Lam
Greg Luri
Ahmad Mahinfallah
Wayne Manges
Pierre Martin
Thomas McCarthy
John McDonald
Jerry Murphy
R. Murphy
Bruce Muschlitz
Charles Ngethe
Joe Nims
Donald Parker
Bansi Patel
Donald Platts
Ulrich Pohl
Craig Preuss
R. Ray
Michael Roberts
Robert Robinson
Jeff Rockower
Charles Rogers
Steven Sano
Sergio Santos
Bartien Sayogo
Thomas Schossig
Samuel Sciacca
Hamid Sharifnia
Devki Sharma
Mark Simon
David Singleton
John Spare
Scott Sternfeld
Gary Stoedter
Eugene Stoudenmire
Walter Struppler
Chandrasekaran Subramaniam
William Taylor
John Tengdin
David Tepen
Eric Thibodeau
Joe Uchiyama
Dmitri Varsanofiev
John Vergis
Jane Verner
Ilia Voloh
Solveig Ward
Kenneth White
Francisc Zavoda
Daidi Zhong

Introduction

This introduction is not part of IEEE Std 1686™-2013, IEEE Standard for Intelligent Electronic Devices Cyber Security Capabilities.

Critical infrastructure protection (CIP) programs developed by utilities are highly dependent on the functionality and capabilities of intelligent electronic devices (IEDs) in regards to cyber security. This standard provides utilities that develop such programs the ability and assurance to procure, install, and commission IEDs that do not compromise their programs. The standard also provides the required suite of functions and capabilities to the various vendors that will be required to incorporate these features in their product line for customers that cite this standard.

Contents

IEEE Standard for Intelligent Electronic Devices Cyber Security Capabilities

IMPORTANT NOTICE: IEEE Standards documents are not intended to ensure safety, health, or environmental protection, or ensure against interference with or from other devices or networks. Implementers of IEEE Standards documents are responsible for determining and complying with all appropriate safety, security, environmental, health, and interference protection practices and all applicable laws and regulations.

This IEEE document is made available for use subject to important notices and legal disclaimers. These notices and disclaimers appear in all publications containing this document and may be found under the heading "Important Notice" or "Important Notices and Disclaimers Concerning IEEE Documents." They can also be obtained on request from IEEE or viewed at http://standards.ieee.org/IPR/disclaimers.html.

1. Overview

1.1 Scope

The standard defines the functions and features to be provided in intelligent electronic devices (IEDs) to accommodate critical infrastructure protection (CIP) programs. The standard addresses security regarding the access, operation, configuration, firmware revision, and data retrieval from an IED. Encryption of communications to and from the IED is also addressed.

1.2 Purpose

The standard defines the functions and features to be provided in IEDs to accommodate CIP programs. Specifically, the standard states what safeguards, audit mechanisms, and alarm indications shall be provided by the vendor of the IED with regard to all activities associated with access, operation, configuration, firmware revision, and data retrieval from an IED. The standard also allows the user to define a security program around these features and alert the user if an IED does not meet this standard as to the need for other defensive measures (technical and/or procedural) that may need to be taken. The encryption for the secure transmission of data to the IED is also part of this standard.

1.3 Reason

The North American Electric Reliability Corporation (NERC) has issued a series of cyber security standards for CIP which, depending on the CIP program at a utility, may drive requirements for cyber security features in some IEDs. Without a clearly defined standard of security features, including their functionality, an owner may unwittingly compromise a corporate CIP program by the deployment of an IED with assumed features that are inconsistent with the user's intentions/assumptions. Stakeholders for the project include the following:

- Utilities/users who can specify that IEDs meet this standard consistent with their CIP programs
- Vendors who will have a clear understanding of the functions and features that must be present in their product offerings
- Regulatory agencies and governments with a vested interest in CIP program effectiveness

In addition to requirements for basic regulatory compliance with NERC CIP standards, utilities should always implement a security strategy for digital assets, including protection and control systems that follow so-called "best practices" from the information technology (IT) industry. The rationale is to protect the bulk power delivery system from compromise and guard utilities against embarrassment, loss of revenue, and potential litigation caused by customer interruption from security breaches.

2. Normative references

The following referenced documents are indispensable for the application of this document (i.e., they must be understood and used, so each referenced document is cited in text and its relationship to this document is explained). For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments or corrigenda) applies.

IEEE Std C37.231™, IEEE Recommended Practice for Microprocessor-Based Protection Equipment Firmware Control.[1, 2]

IEEE Std 1711™, IEEE Trial-Use Standard for a Cryptographic Protocol for Cyber Security of Substation Serial Links.

NIST Cryptographic Toolkit.[3]

3. NIST Cryptographic Toolkit acronyms

For the purposes of this document, the following acronyms apply. The *IEEE Standards Dictionary Online* should be consulted for acronyms and terms not defined in this clause.[4]

CIP	critical infrastructure protection
HTTPS	Hypertext Transfer Protocol Secure

---

[1] The IEEE standards or products referred to in this clause are trademarks of The Institute of Electrical and Electronics Engineers, Inc.
[2] IEEE publications are available from The Institute of Electrical and Electronics Engineers, 445 Hoes Lane, Piscataway, NJ 08854, USA (http://standards.ieee.org/).
[3] Available at: http://csrc.nist.gov/groups/ST/toolkit/index.html
[4] *IEEE Standards Dictionary Online* subscription is available at: http://www.ieee.org/portal/innovate/products/standard/standards_dictionary.html.

ID	identification
IED	intelligent electronic device
IT	information technology
LAN	local area network
NERC	North American Electric Reliability Corporation
NTP	Network Time Protocol
RBAC	role-based access control
SCADA	supervisory control and data acquisition
SFTP	secure file-transfer protocol
SNMP	Simple Network Management Protocol
SSH	secure shell
TCP	Transfer Control Protocol
TOC	table of compliance
UDP	User Datagram Protocol
VPN	virtual private network
WAN	wide area network

4. Use of this standard

4.1 General

The purpose of this standard is to establish a baseline of security requirements and features to be provided in electric utility IEDs. The use of this standard in the procurement and testing of IEDs may help ensure that a cyber security program that requires specific compliance to IEEE Std 1686™ table of compliance (TOC) features is not compromised by the lack of a required feature or an operation in an unintended manner when new IEDs are installed. For users who make this standard an integral part of their IED cyber security posture, it is important to note the following:

CAUTION

Adherence to this standard does not ensure adequate cyber security.

Successful cyber security of IEDs is a combination of technology, administrative procedures, documentation, monitoring, and diligent enforcement. IED cyber security technology alone will not accomplish effective cyber security if other elements are not in place such as:

- Control and monitoring of physical access to the secure perimeter housing the IED
- IED password administration
- Control of sensitive IED documents (technical manuals, schematics, etc.)
- Real time monitoring of IED conditions and alarming
- Security awareness training of utility personnel
- Security plans and procedures for non-utility personnel (system integrators, panel suppliers, contract maintenance suppliers, etc.)
- Control of sensitive drawings and files

It is also important to note that adherence to every subclause of this standard may not be required for a specific cyber security program. Users may elect to implement procedural and administrative elements of a cyber security program that may serve to make elements of this standard redundant and/or superfluous. For example, some IEDs can have electronic access remotely enabled and disabled through supervisory control and data acquisition (SCADA). For these devices, implementing a verifiable manual access request procedure (e.g., a verbal request to the SCADA control center) may eliminate the need for unique user ID/passwords for electronic access and the IED features associated with password administration would not be required in that security program.

This standard provides a set of features, functions, and practices for IEDs and IED configuration software that is deemed to require security for electronic access (local or remote) for functions such as:

- Configuration
- Data access
- Diagnostics
- Firmware upgrades
- Configuration software upgrade
- Manually forced data or operation

A cyber security program can use this standard to assess how new or existing IEDs meet the significant security issues addressed in this standard. The fact that a new or existing IED does not meet this standard does not imply that an effective security program is not capable of securing the IED per a particular security program's requirements. In this case, this standard will help users identify what features a separate system should have in order to raise the security level of an IED.

4.2 Applicability

This standard can be applied to any IED. Although the standard is designed to provide the tools and features for a user to implement an IED security effort in response to NERC CIP requirements [B5][5], the standard is applicable to any IED where the user requires security, accountability, and auditability in the configuration and maintenance of the IED.

This standard does not address which devices should be required to meet the standard. Each user must assess their specific situation and choose where the standard should apply in their particular case. Issues affecting this choice include, but are not limited to, the following:

---

[5] The numbers in brackets correspond to those of the bibliography in Annex B.

- IED classification (critical/non-critical infrastructure)
- User’s cyber security plan and procedures
- Communication and local area network (LAN)/wide area network (WAN) facilities
- Protection and control system architecture

4.3 Implementing IED security

The implementation of a security posture for IEDs and their configuration software is a combination of technology and procedures. Technology alone will not produce the desired results without the implementation and enforcement of a set of complementary security procedures. Additionally, security procedures and technology are often developed in conjunction with one another with considerations given to such things as operational costs, user practices, manpower constraints, and communications capabilities.

This standard defines the functions and features to be provided in IEDs to accommodate CIP programs. It is recognized, however, that in some cases, the functions and features may require some adaptation or relaxation to meet a user’s specific situation. As an example, this standard calls for at least ten unique userID/passwords for the IED. In a very small utility such as a municipality, there may not be ten users who require access, and therefore the requirement is not substantiated. For a very large utility with an IED maintenance force that covers a wide geographical area, ten individual passwords may not be enough. In such cases, the user must identify to the IED provider where the user’s requirements differ or exceed the standard.

Further, the failure of an IED to meet every clause of this standard does not necessarily preclude its use in a secure environment. It is possible the deficiency may be overcome by procedural or administrative technology, architecture, or other measures.

4.4 Proper use of this standard

4.4.1 IEEE Std 1686 requirements

The proper use of this standard requires the following three elements:

a) Proper citation of the standard
b) TOC to the standard
c) Analysis and verification by the user of the IED offering

4.4.2 Proper citation

The proper citation of this standard in a procurement document is as follows:

> The IED shall meet or exceed the requirements established in IEEE Std 1686, Standard for Intelligent Electronic Devices Cyber Security Capabilities.

Modifications to the standard by the user to meet specific circumstances or requirements of the user are permissible, so long as they are clearly identified in supporting documentation that accompanies the specification as part of a procurement process. When this is desired, it may be stipulated in a citation as in the following examples:

> The IED shall meet or exceed the requirements established in IEEE Std 1686, Standard for Intelligent Electronic Device Cyber Security Capabilities, except as noted below:
>
> 5.1.3: The minimum number of passwords shall be 20 (user desires a greater number of passwords than provided by the standard)
>
> 5.2.1: The minimum number of records in the audit trail shall be 512 (user desires to relax the number of audit trail records required in the standard to be retained by the IED)

Users are strongly discouraged against making generic statements such as "IED shall meet all applicable clauses and subclauses of IEEE Std 1686." Such statements create the potential for differing assessments by the user and the vendor/supplier as to what is applicable.

4.4.3 Table of compliance (TOC)

Vendors/suppliers who are claiming compliance with this standard shall be required to provide a TOC. The TOC shall list every subclause of Clause 5 of this standard on a separate line. For each subclause, the vendor/supplier shall then indicate the level of compliance for the product in question. The following responses shall be used:

- Acknowledge: Used as a placeholder when no requirement is presented in the subclause
- Exception: Product fails to meet one or more of the stated requirements of the subclause
- Comply: Product fully meets the stated requirements of the subclause
- Exceed: Product exceeds one or more of the stated requirements of the subclause

A column for comments and explanations may be included to provide additional information the vendor deems useful for clarification of the response.

An example of a TOC is shown in Annex A.

5. IED cyber security features

5.1 Electronic access control

5.1.1 IED access control overview

All electronic access to the IED, whether locally through a control panel, locally through a communication/diagnostic port with a test set or personal computer, or remotely through communications media, shall be protected by unique user identification (ID) and password combinations. Once a user has configured a proper ID/password combination, it shall not be possible to gain access to the device without a proper ID/password combination that has been generated by the user.

The IED shall have an open and documented interface to change user accounts, passwords, and roles, which can be enacted through the use of a third party products (for example, a centralized batch process system).

5.1.2 Password defeat mechanisms

The IED shall have no means, undisclosed to the implementing entity, whereby the user-created ID/password control can be defeated or circumvented. This includes, but is not limited to the following mechanisms and techniques:

- Embedded master password
- Chip-embedded diagnostic routines that automatically run in the event of hardware or software failures
- Hardware bypass of passwords, such as jumpers and switch settings

The vendor shall disclose any and all mechanisms whereby the user-created ID/password control can be circumvented. If the vendor represents that no such mechanisms are present in the IED, the vendor shall certify in writing to that effect.

5.1.3 Number of individual users

The minimum number of individual users supported by the IED shall be ten.

5.1.4 Password construction

User-created passwords shall follow a set of rules that shall be adhered to in the creation of each password. At least eight characters shall be used, and the password shall be case sensitive. When encoding passwords in plain text, the password characters shall contain the following:

- At least one uppercase and one lower case letter
- At least one number
- At least one non-alphanumeric character (e.g., @, %, &, *)

Any attempt to create a password that violates these rules shall be captured at the time of attempted creation, and the user shall be notified and prompted to choose another password that conforms to the rules.

5.1.5 IED access control

5.1.5.1 Authorization levels by password

The IED shall support the ability to assign authorization to utilize one or more IED functions and features based on individual user-created ID/password combinations. At the least, the functions and features listed in 5.1.6 a) through 5.1.6 g) shall have this assignability available. For additional functions not listed in 5.1.6 a) through 5.1.6 g), ID/password capability shall be documented.

5.1.5.2 Authorization using role-based access control (RBAC)

The IED shall have the capability of defining at least four user-defined roles. Each role shall have the capability of having any combination of functions listed in 5.1.6 a) through 5.1.6 g) assigned to that role. A role shall be assignable to each user/password combination, thereby conveying the permissions of that role to the user upon log in.

5.1.6 IED main security functions

The IED main security functions include the following:

a) View data refers to the ability to view operational data (voltage, current, power, energy, status, alarms, et al.) of the IED that are not intended to be available as general information display.

b) View configuration settings refer to the ability to view configuration settings of the IED, such as scaling, communications addressing, programmable logic routines, and the firmware version numbers.

c) Force values refer to the ability to manually override real data with manually inputted data and/or the ability to cause a control-output operation to occur.

d) Configuration change refers to the ability to download and upload configuration files to the unit and/or effect changes to the existing configuration.

e) Firmware change refers to the ability to load new firmware that does not require a corresponding hardware change.

f) ID/password or RBAC management refers to the ability to create, delete, or modify user IDs, passwords, roles and/or password, and role authorization levels.

g) Audit trail refers to the ability to view and download the audit trail.

5.1.7 Password display

Only user IDs shall be displayed in screens, audit trails, the memory area or files, and other records and configuration files. It shall not be possible to cause IED passwords to be displayed through any means, including local display panel, configuration software (local or remote; offline or online), web browser, and terminal access.

5.1.8 Access timeout

The IED shall have a timeout feature that automatically logs out a user who has logged in after a period of user inactivity. Inactivity shall be defined as the absence of input from local (faceplate) mechanisms and/or the absence of keystroke activity on a computer connected to the IED port. The period of time before the timeout feature activates shall be settable between 1 min and 60 min in 1-min intervals by the user in the configuration of the IED.

5.2 Audit trail

5.2.1 Audit trail background

The IED shall record in a sequential circular buffer (first in, first out), an audit trail (audit log) listing events of 5.2.4 in the order in which they occur.

There shall be no capability to erase or modify the audit trail as it shall keep full integrity for audit purposes.

5.2.2 Storage capability

The audit trail facility shall store at least 2048 events before the circular buffer begins to overwrite the oldest event with the newest event. It shall not be possible to remove the storage media of the audit trail without permanently damaging the IED beyond the capability of field repair.

5.2.3 Storage record

For each audit trail event, the following information shall be recorded:

a) Event record number: The automatically-generated sequential number for the event
b) Time and date: Time and date of the event including year, month, day, hour, minute, and second
c) User identification: The user ID logged into the IED at the time of the event
d) Event type: Reference 5.2.4 below for a definition of event types

5.2.4 Audit trail event types

The following events shall cause an entry into the Audit Trail record:

a) Log in: Successful log in (locally or remotely) of a user to the device
b) Manual log out: User-initiated log out
c) Timed log out: Log out of user after a predefined period of inactivity elapses
d) Value forcing: Action of a logged in user which overrides real data with manual entry and/or causes a control operation
e) Configuration access: Downloading of a configuration file from the IED to an external device or memory location (e.g., computer, memory stick, compact disk)
f) Configuration change: The uploading of a new configuration file to the IED or keystroke entry of new configuration parameters that causes a change in IED configuration
g) Firmware change: Writing to memory of new IED operating firmware
h) ID/password creation or modification: Creation of new ID/password or modification of ID/password or RBAC levels of authorization
i) ID/Password deletion: Deletion of a user ID/password
j) Audit log access: User access of audit log for viewing or audit log download to an external device or memory location (e.g., computer, memory stick, compact disk)
k) Time/date change: User request to change time and date
l) Alarm incident: The occurrence of an alarm incident as defined in 5.3.3

5.3 Supervisory monitoring and control

5.3.1 Overview of supervisory monitoring and control

In addition to the audit trail capability, the IED shall monitor security-related activity and shall make the information available through a real-time communication protocol for transmission to a supervisory system. The supervisory system shall be either a SCADA system or network management system. If serial communications are used for the configuration of the IED and the supervisory communications port, separate serial communications ports shall be provided for configuration and supervisory monitoring. Configuration port activity shall not interfere with nor disable the supervisory monitoring port, with the exception of a configuration or firmware change requiring a reboot of the IED.

Information to be monitored and transmitted shall fall into two groups: events and alarms.

5.3.2 Events

Events are defined as authorized activities which can be expected to occur in the routine use and maintenance of the IED. All events listed in 5.2.4 shall be included in the requirement for events to be monitored and transmitted to the supervisory system.

Event points shall have momentary change detect capability so that the occurrence of an event will be reported on the next scan of the IED by the supervisory system. The IED shall report each occurrence as an individual event.

5.3.3 Alarms

Alarms are defined as activities which may indicate unauthorized activity. The following shall cause a unique alarm occurrence:

a) Unsuccessful login attempt: Three incorrect password entries in succession during a single log-in attempt. Successive failed log-in attempts after three shall generate a single entry into the audit trail listing the time of the last attempt and total number of log-in attempts that have occurred in succession.
b) Reboot: The rebooting or restarting of the IED by means of removing power or through the use of a device-resident rebooting mechanism such as a reset button, power-up sequence, or access software feature.
c) Attempted use of unauthorized configuration software: The detection by the IED of an attempted use of configuration software, accessing computer, or a combination thereof that is not registered as legitimately able to be used for configuration of the IED.
d) Invalid configuration or firmware download: The detection by the IED of a configuration or firmware download to the IED that does not contain the proper credentials that identify the configuration or firmware as valid.
e) Unauthorized configuration or firmware file: The detection by the IED of a configuration or firmware download to the IED that does not contain the proper credentials that identify the configuration or firmware as authorized.
f) Time signal out of tolerance: The IED shall validate time synchronization messages received through protocol or dedicated time synchronization channels and alarm if the time synchronization message is not within the tolerances of the IED's internal/local clock.
g) Invalid field hardware changes: The IED shall validate user-performable (as identified by the vendor) field hardware changes and alarm if the field hardware change is performed improperly (i.e., wrong I/O board inserted in a designated I/O slot).

5.3.4 Alarm point change detect

Alarm points shall have momentary change detect capability so that the occurrence of an alarm will be reported on the next scan of the IED by the supervisory system. The IED shall report each occurrence as an individual alarm.

5.3.5 Event and alarm grouping

A means shall be provided to allow the user to group events and alarms. If a point is assigned to a group, only the group alarm shall be sent to the supervisory system upon the occurrence of that point. Individual points shall be assignable to a group in any combination.

Assigning points to a group for supervisory reporting shall not cause the individual point identification in the audit trail to be affected.

At least two groups shall be provided. One group shall be for events and the other group shall be for alarms.

Group events and alarms shall have momentary change detect capability so that the occurrence of a group event or group alarm will be reported on the next scan of the IED by the supervisory system.

5.3.6 Supervisory permissive control

The IED shall provide a mechanism that, when enabled, requires independent supervisory permission prior to performing actions or requests in the field and/or remotely. Permissions shall be effected by the operation of pseudo control points issued by the master station of the supervisory system.

All diagnostic ports shall have the ability to be enabled and disabled remotely through a supervisory control command. If enabled, the port shall have the capability of being disabled in the following manner:

- Manually, upon command from the supervisory system
- Automatically, upon detection of the IED of an alarm event (5.3.3)
- Automatically in the event that a successful log-in does not take place after enabling the port within a time period configurable from 1 min to 60 min in 1-min increments

At the least, the features identified in 5.2.4 shall be assignable to require supervisory permissive control.

At least three permission levels shall be provided. The IED shall provide the mechanism to allow any feature to be assigned to one, two, or all three permission levels on an individual password or role basis.

5.4 IED cyber security features

5.4.1 IED functionality compromise

The general purpose of this subclause is to alert the user of any possible compromise of the primary IED functions during the usage of either the protocol port(s) or diagnostic port(s). The IED vendor shall specifically state what functions, if any, may be affected by usage of any protocol or diagnostic port.

5.4.2 Specific cryptographic features

For IEDs that implement specific communications functions over IP-based networks, the following cryptographic techniques and versions shall be implemented in the IED:

a) Webserver functionality provided by the IED shall be Hypertext Transfer Protocol Secure (HTTPS).

b) File transfer functionality provided by the IED shall be Secure File-Transfer Protocol (SFTP).

c) Text-oriented communication facilities using a virtual terminal connection over an Ethernet-based network shall be secure shell (SSH).

d) Single Network Management Protocol (SNMP) implemented in the IED shall be SNMPv3.

e) Network time synchronization shall be Network Time Protocol (NTP). Network time synchronization functionality implemented by NTP shall be NTP v3/4 or SNTP 3/4.

f) Secure tunnel functionality provided by the IED shall be a virtual private network (VPN).

5.4.3 Cryptographic techniques

There are numerous cryptographic techniques, and combinations of techniques that can be employed in a cyber security program to achieve secure communications between IEDs. One or more of these techniques may be implemented by an IED vendor as product features of the IED. These techniques include the following:

- Block ciphers
- Block cipher modes
- Digital signatures
- Entity authentication
- Key derivation functions
- Message authentication
- Random number generation
- Secure hashing
- Key establishment

IEDs that offer any of the above listed cryptographic features shall be compliant with the requirements specified by the NIST Computer Security Division.

Because the techniques and versions of techniques might change in response to new cryptographic discoveries, technological advances or threats, IEDs shall comply with the current NIST requirements at the time they are manufactured.

5.4.4 Encrypting serial communications

IEDs that are able to employ serial communications for any remote access application (data transfer, configuration, firmware upload, etc.) shall provide data encryption in accordance with IEEE Std 1711[6] for all ports designed to permit remote access.

5.4.5 Protocol-specific security features

For whichever protocols are implemented in the IED, the corresponding security controls of those protocols shall likewise be implemented in the IED.

---

[6] Information on references can be found in Clause 2.

5.5 IED configuration software

5.5.1 Authentication

The IED shall have a means to authenticate that the configuration software being used to access or change the configuration is a copy that has been authorized by the user. Unauthorized copies of the configuration software shall be prevented from accessing any features of the IED.

5.5.2 Digital signature

The configuration software shall have the capability to generate a digital signature in the configuration and firmware download files indicating the file has been produced by an authorized configuration software program and by an authorized user. The IED shall have the capability to read the digital signature applied to a configuration file or firmware file to verify that the file has been created by an authorized entity and has not been altered or corrupted. The IED shall only accept properly signed files.

5.5.3 ID/password control

The configuration software shall be ID/password controlled so that the software cannot be accessed without the proper ID/password combination. At least ten individual ID/password combinations shall be provided for each copy of the configuration software program. Under no circumstances shall the configuration software cause the passwords of the software itself or the IED to be displayed in readable text.

5.5.4 ID/password controlled features

IED configuration software shall have the ability to assign features to specific users and/or roles. At the least, the functions and features outlined in 5.5.4.1 and 5.5.4.2 shall be assignable on an individual user or role basis.

5.5.4.1 View configuration data

In view configuration data mode, a user can only view configuration data. No changes to the configuration can be made.

5.5.4.2 Change configuration data

In change configuration data mode, the user can change and save configuration data and/or firmware revision files to be uploaded to the IED at a later point in time.

a) Full access: In full access mode, all functions, including ID/password changes and user assignment levels can be made.
b) Change tracking: The configuration tool shall provide change tracking of any and all changes to the IED configuration.
c) Use monitoring: The configuration tool shall log when a user begins and ends using the tool.
d) Download to IED: The configuration tool shall log when a user applies (downloads) a configuration and or firmware revision to an IED.

5.6 Communications port access

All communications ports, whether physical or logical, other than the diagnostic port on the IED shall have the capability to be enabled or disabled through configuration of the IED. When disabled through configuration, no communications shall be possible through the disabled port.

The IED shall have all User Datagram Protocol (UDP) and Transmission Control Protocol (TCP) ports that are not being used by an application disabled.

5.7 Firmware quality assurance

Firmware quality assurance shall be in compliance with IEEE Std C37.231, Recommended Practice for Microprocessor-Based Protection Equipment Firmware Control.

Annex A

(informative)

Table of Compliance (TOC)

Table A.1 is an example TOC for a hypothetical device. It is shown to illustrate the proper construction of the table and to indicate the possible range of responses that might be expected from a vendor who is citing compliance for its product to this standard.

Table A.1—Table of compliance

Clause number	Clause/subclause title	Status	Comment
5	IED cyber security features	Acknowledge	
5.1	Electronic access control	Comply	
5.1.2	Password defeat mechanisms	Comply	
5.1.3	Number of individual users	Exceed	Product provides for 25 individual ID/password combinations
5.1.4	Password construction	Exception	Upper and lower case letters are interchangeable. Non-alphanumeric characters cannot be used in password
5.1.5	IED access control	Acknowledge	
5.1.5.1	Authorization levels by password	Comply	
5.1.5.2	Authorization using role-based access control (RBAC)	Exceed	Product provides six user-defined roles
5.1.6	IED main security functions	Acknowledge	
5.1.6 a)	View data	Comply	
5.1.6 b)	View configuration settings	Comply	
5.1.6 c)	Force values	Exception	Feature not supported on this product
5.1.6 d)	Configuration change	Comply	
5.1.6 e)	Firmware change	Comply	
5.1.6 f)	ID/password or RBAC management	Comply	
5.1.6 g)	Audit trail	Comply	
5.1.7	Password display	Comply	
5.1.8	Access timeout	Exception	Timeout period is set by a jumper on the main board. Possible selections are 1 min, 5 min, 10 min, 30 min, and 60 min
5.2	Audit trail	Comply	
5.2.2	Storage capability	Exceed	Audit trail supports 4096 events before overwrite
5.2.3	Storage record	Comply	
5.2.3 a)	Event record number	Comply	
5.2.3 b)	Time and date	Exceed	User can define the format of the date
5.2.3 c)	User identification	Comply	
5.2.3 d)	Event type	Comply	
5.2.4	Audit trail event types	Comply	
5.2.4 a)	Log in	Comply	
5.2.4 b)	Manual log out	Comply	
5.2.4 c)	Timed log out	Comply	
5.2.4 d)	Value forcing	Comply	
5.2.4 e)	Configuration access	Comply	
5.2.4 f)	Configuration change	Comply	
5.2.4 g)	Firmware change	Exception	Firmware changes are not captured in the audit trail record
5.2.4 h)	ID/password creation or modification	Comply	

Table A.1—Table of compliance *(continued)*

Clause number	Clause/Subclause Title	Status	Comment
5.2.4 i)	Password deletion	Comply	
5.2.4 j)	Audit log access	Comply	
5.2.4 k)	Time/date change	Comply	
5.2.4 l)	Alarm incident	Comply	
5.3	Supervisory monitoring and control	Comply	
5.3.2	Events	Comply	
5.3.3	Alarms	Comply	
5.3.3 a)	Unsuccessful login attempt	Exception	Alarm is set after six unsuccessful attempts within a 5-min period
5.3.3 b)	Reboot	Exception	A specific alarm for a reboot is not available. However, user can deduce that a reboot has taken place by examining the DNP3.0 initialization bit being set followed by a DNP3.0 request for time.
5.3.3 c)	Attempted use of unauthorized configuration software	Comply	
5.3.3 d)	Invalid configuration or firmware download	Comply	
5.3.3 e)	Unauthorized configuration or firmware file	Comply	
5.3.3 f)	Time signal out of tolerance	Comply	
5.3.3 g)	Invalid field hardware changes	Comply	
5.3.4	Alarm point change detect	Comply	
5.3.5	Event and alarm grouping	Exceed	Three groups are provided: “Critical Alarms,” “Alarms,” and “Events”
5.3.6	Supervisory permissive control	Comply	
5.4	IED cyber security features	Acknowledge	
5.4.1	IED functionality compromise	Comply	Download of configuration will disable all other operations during the period of download
5.4.2	Specific crytographic features	Acknowledge	
5.4.2 a)	Webserver functionality	Comply	Feature not offered in this product
5.4.2 b)	File transfer functionality	Comply	
5.4.2 c)	Text-oriented terminal connections	Comply	
5.4.2 d)	SNMP network management	Exception	SNMPv2 implemented in this product
5.4.2 e)	Network time synchronization	Exception	IEEE Std C37.238 implemented in this product
5.4.2 f)	Secure tunnel functionality	Comply	
5.4.3	Cryptographic techniques	Comply	
5.4.4	Encrypting serial communications	Comply	
5.4.5	Protocol-specific security features	Comply	
5.5	IED configuration software	Acknowledge	
5.5.1	Authentication	Exception	Feature not supported
5.5.2	Digital signature	Comply	
5.5.3	ID/password control	Exception	Passwords can be viewed in the configuration by someone with Supervisor Level Authority
5.5.4	ID/password controlled features	Comply	
5.5.4.1	View configuration data	Comply	
5.5.4.2	Change configuration data	Comply	
5.5.4.2 a)	Full access	Comply	
5.5.4.2 b)	Change tracking	Comply	
5.5.4.2 c)	Use monitoring	Comply	
5.5.4.2 d)	Download to IED	Comply	
5.6	Communications port access	Comply	
5.7	Firmware quality control	Comply	

Annex B

(informative)

Bibliography

Bibliographical references are resources that provide additional or helpful material but do not need to be understood or used to implement this standard. Reference to these resources is made for informational use only.

[B1] Accredited Standards Committee C2, National Electrical Safety Code® (NESC®).[7]

[B2] IEEE PSRC CI Working Group Report "Cyber Security Issues for Protective Relays."[8]

[B3] IEEE Std C37.1™, IEEE Standard for SCADA and Automation Systems.

[B4] IEEE Std C37.238™, IEEE Standard Profile for Use of IEEE 1588™ Precision Time Protocol in Power System Applications.

[B5] NERC Cyber Security Standards CIP-002 to CIP-009.[9]

[B6] RFC 1157, J. Case, M. Fedor, M. Schoffstall, and J. Davin, eds., "A Simple Network Management Protocol (SNMP)," May 1990.[10]

---

[7] The NESC is available from the Institute of Electrical and Electronics Engineers, 445 Hoes Lane, Piscataway, NJ 08854, USA (http://standards.ieee.org/).

[8] This publication is available from The Institute of Electrical and Electronics Engineers, 445 Hoes Lane, Piscataway, NJ 08854, USA (http://standards.ieee.org/).

[9] Available from http://www.nerc.com.

[10] Available from http://www.ietf.org/rfc/rfc1157.txt.

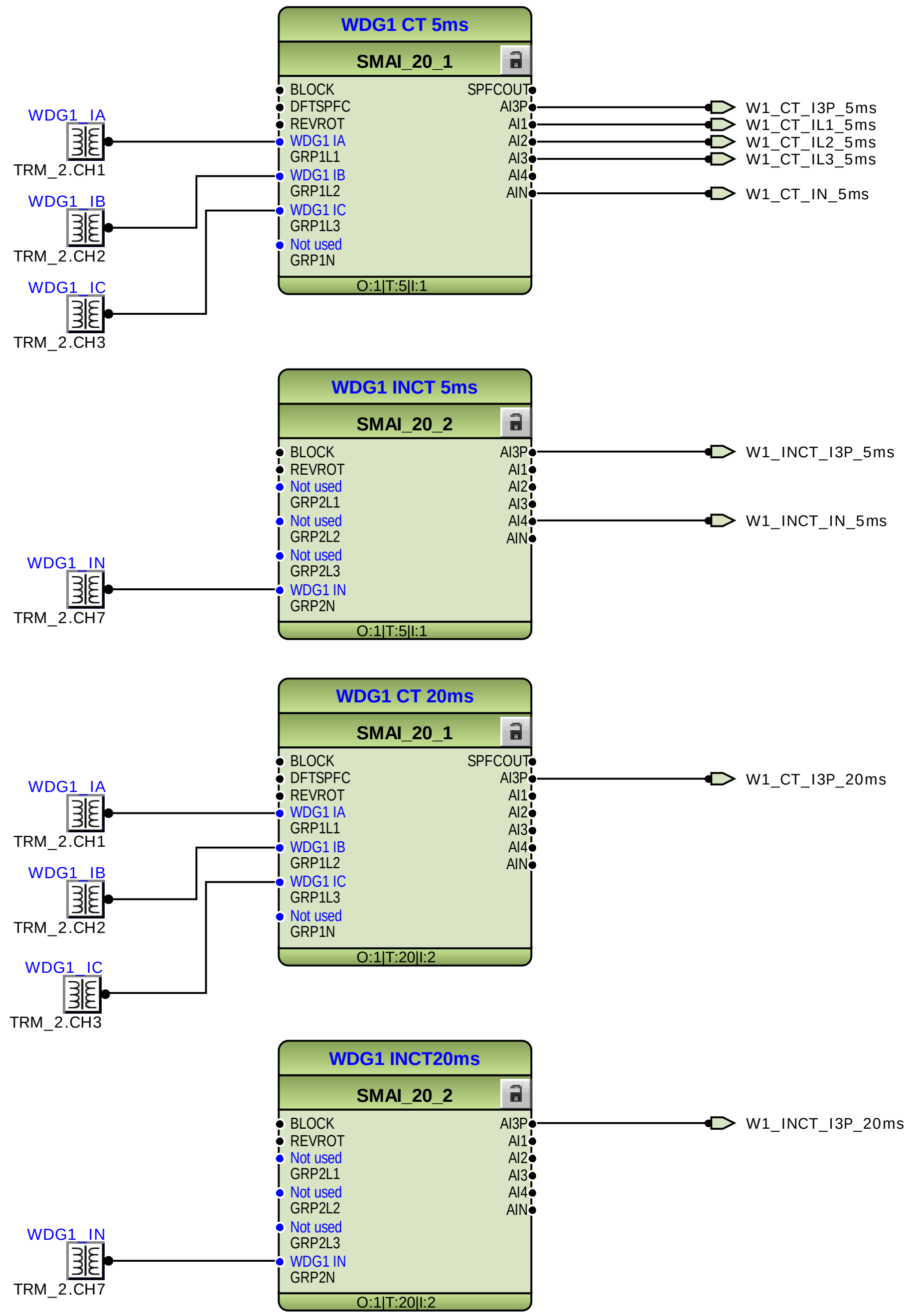
Appendix B: Application Configuration Drawings of IED RET650

RET650 A01A CONFIGURATION

Two winding, Single Breaker

Main Application	Description
OVERVIEW	List of contents
ANALOG_INPUTS	Analog inputs for current and voltage circuits
INPUTS	Function keys, binary inputs and GOOSE receive functions
DIFF_PROT	Differential protection functions
WDG1_PROT	Winding 1 protection functions
WDG2_PROT	Winding 2 protection functions
LOGIC	Signal logic
TRIP	Tripping logic
COND_MON	Condition monitoring and supervision functions
MEASURE	Measurement functions
VOLTAGE_CONTROL	Voltage control functions
OUTPUTS	LEDs, binary outputs and GOOSE send functions
DISTURBANCE_RECORDER	Disturbance report functions
COMMON	General IED functions

					Project Ryerson University	Responsible department ABB Ltd.	Technical reference	Document kind Graphical Application Configuration	Doc. designation AA1J1Q01A3
				Replacing	**Ryerson University** Ryerson University.Substation.Voltage Level.Bay		Created by	Title RET650	Document id.
Rev.	Modification	Rel. date	Created by	Based on			Approved by		Rev. 0 | Rel. date 6/23/2014 | Lang. en | 1 / 10



Main Application: ANALOG_INPUTS, Page: 1

Rev. | Modification | Rel. date | Created by | Replacing | Based on

Project
Ryerson University
Ryerson University
Ryerson University.Substation.Voltage Level.Bay

Responsible department
ABB Ltd.

Technical reference

Created by

Approved by

Document kind
Graphical Application Configuration

Title
RET650

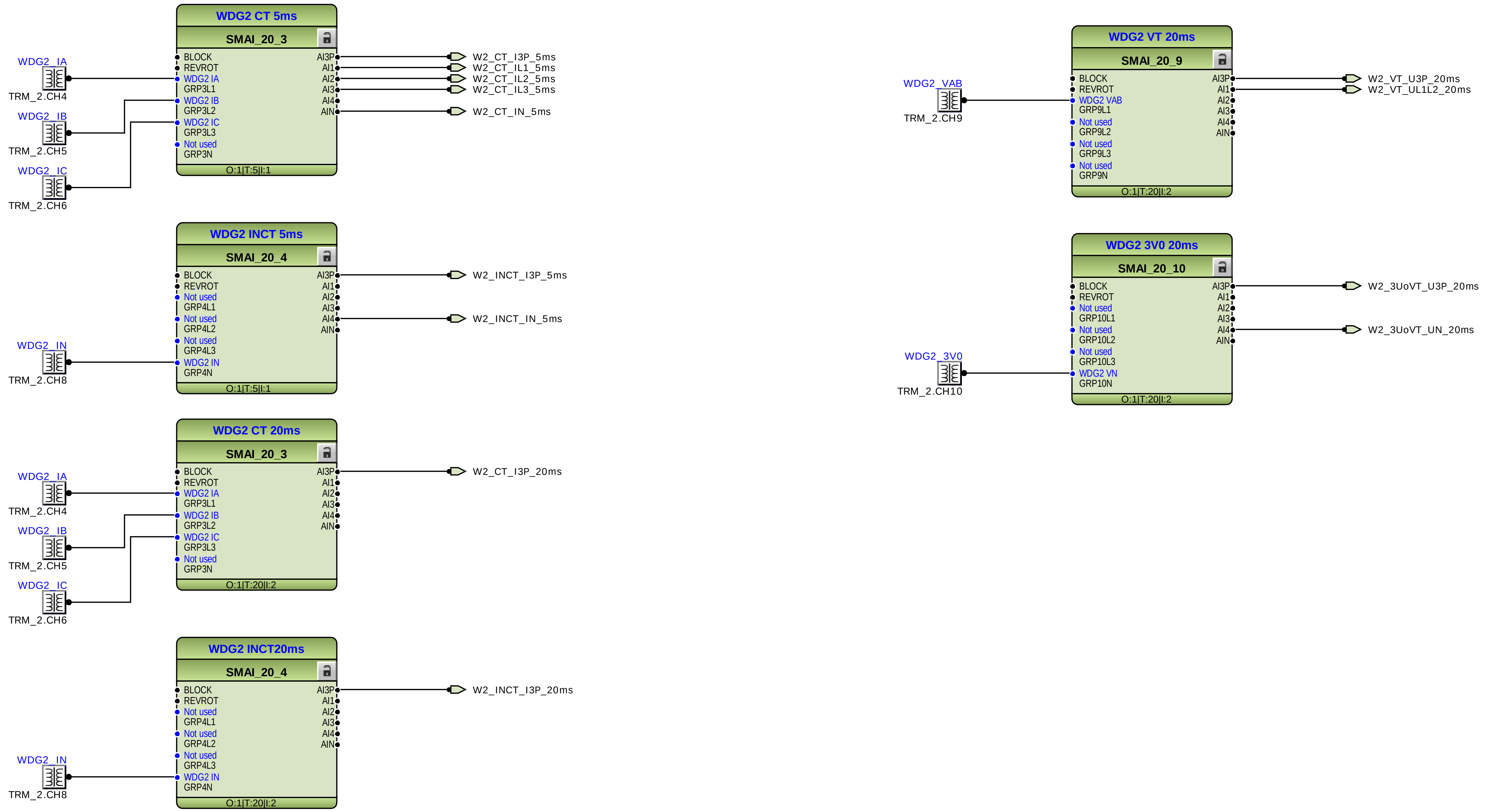
Doc. designation
AA1J1Q01A3

Document id.

Rev.
0

Rel. date
6/23/2014

Lang.
en



Main Application: ANALOG_INPUTS, Page: 2

Project
Ryerson University

Replacing
Ryerson University
Ryerson University.Substation.Voltage Level.Bay

Rev.	Modification	Rel. date	Created by	Based on

Responsible department
ABB Ltd.

Technical reference
Created by
Approved by

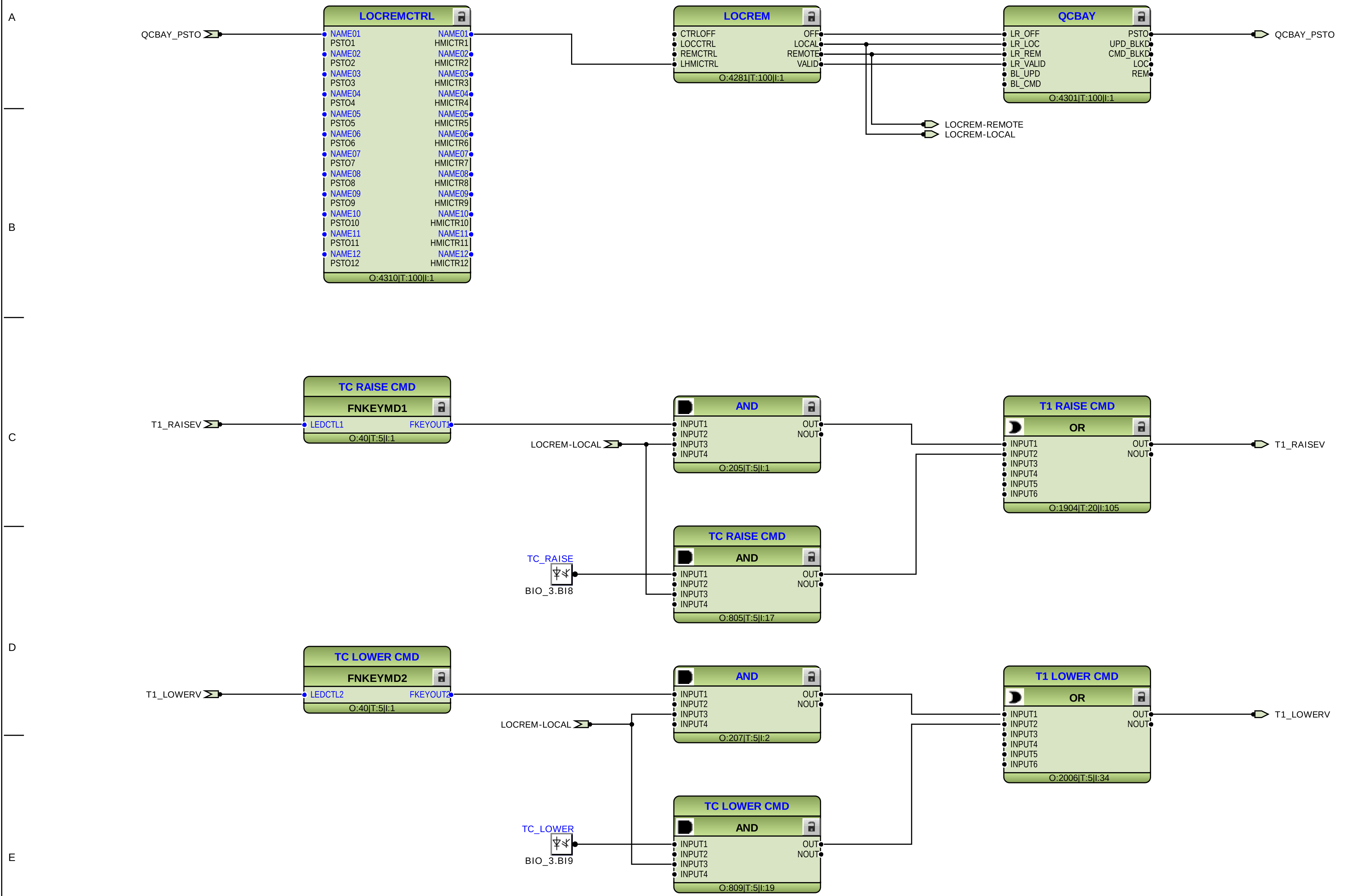
Document kind
Graphical Application Configuration

Title
RET650

Doc. designation
AA1J1Q01A3

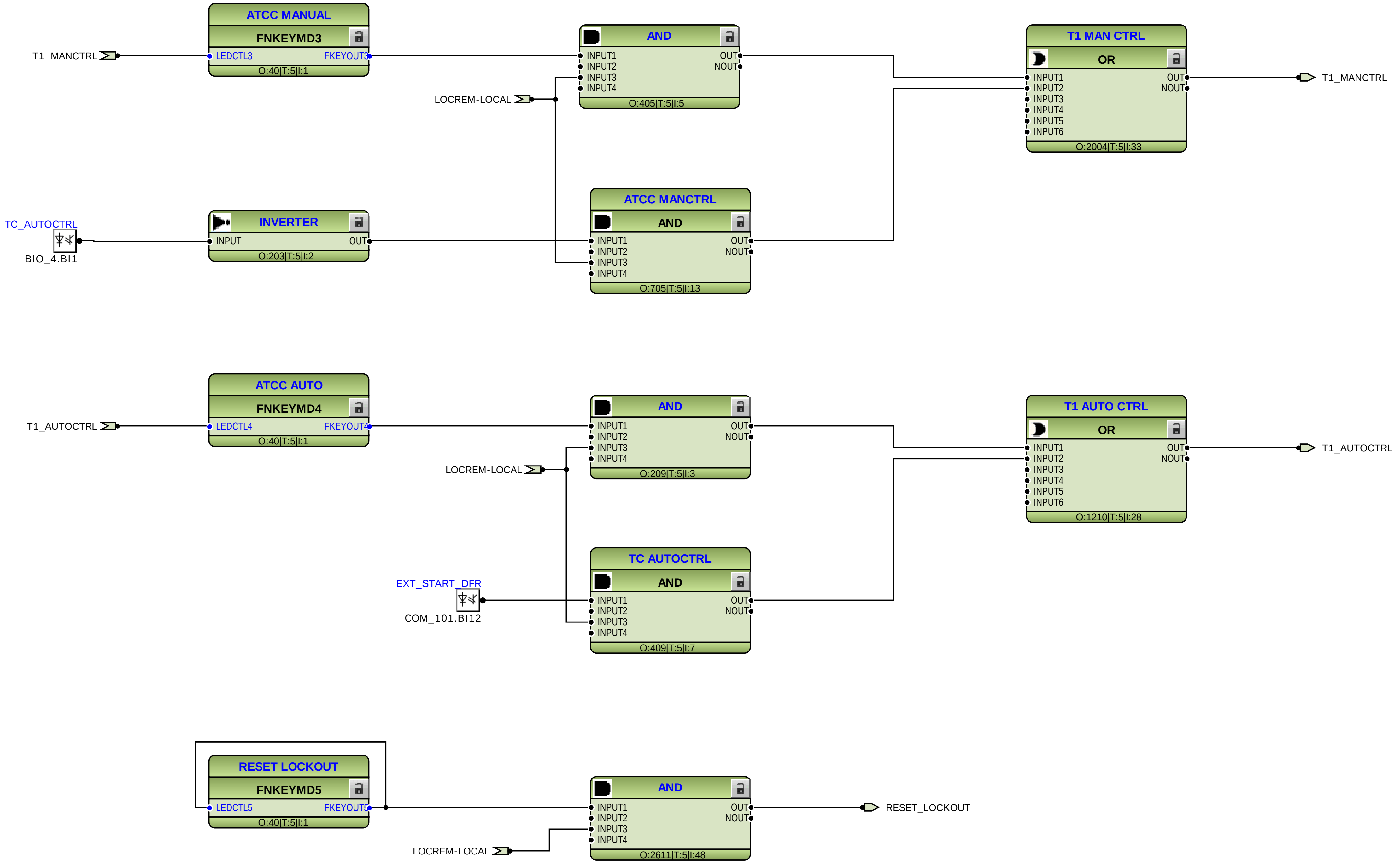
Document id.

Rev.	Rel. date	Lang.	
0	6/23/2014	en	3 / 10



Main Application: INPUTS, Page: 1

				Project Ryerson University	Responsible department ABB Ltd.	Technical reference	Document kind Graphical Application Configuration	Doc. designation AA1J1Q01A3
			Replacing	**Ryerson University** Ryerson University.Substation.Voltage Level.Bay		Created by	Title RET650	Document id.
Rev.	Modification	Rel. date	Created by	Based on		Approved by		Rev. 0 / Rel. date 6/23/2014 / Lang. en



Main Application: INPUTS, Page: 2

Rev. | Modification | Rel. date | Created by | Based on | Replacing

Project
Ryerson University

Ryerson University
Ryerson University.Substation.Voltage Level.Bay

Responsible department
ABB Ltd.

Technical reference

Created by

Approved by

Document kind
Graphical Application Configuration

Title
RET650

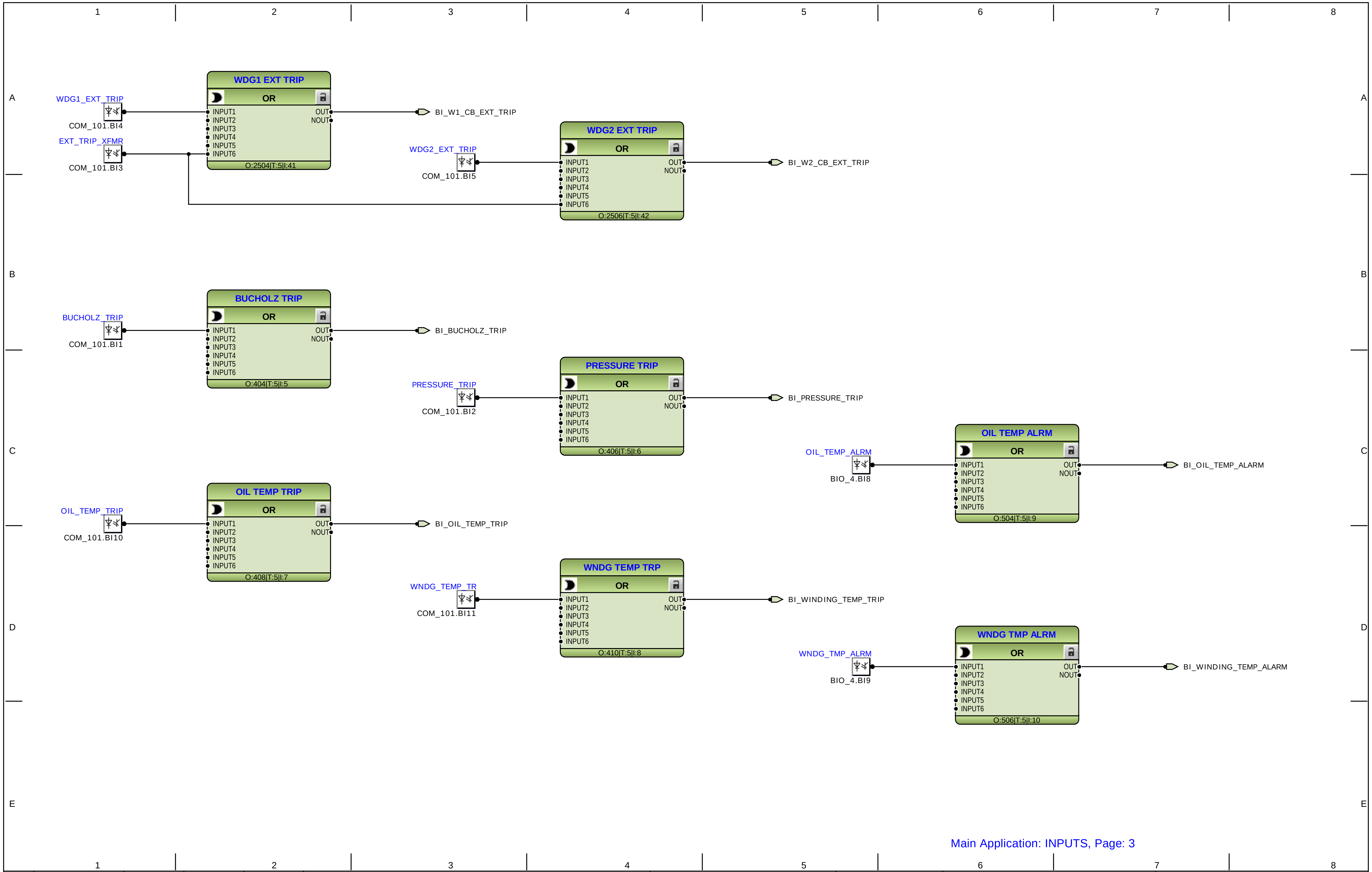
Doc. designation
AA1J1Q01A3

Document id.

Rev.
0

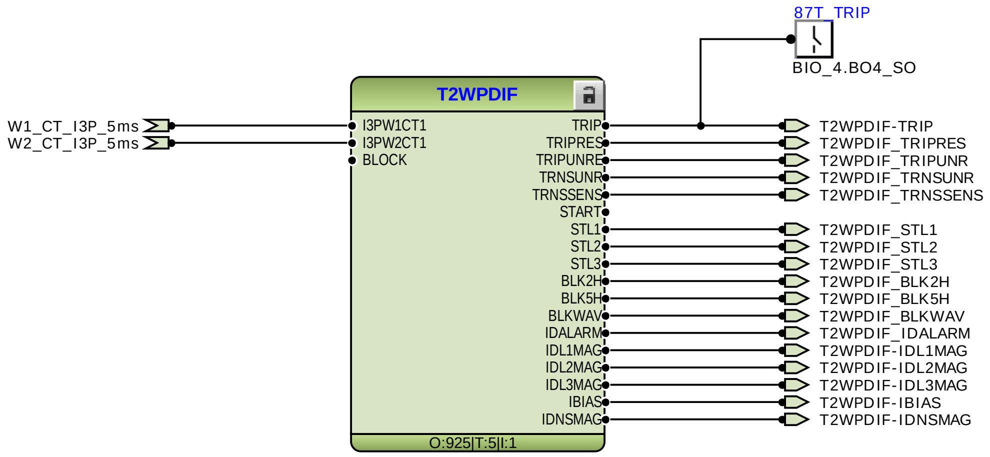
Rel. date
6/23/2014

Lang.
en



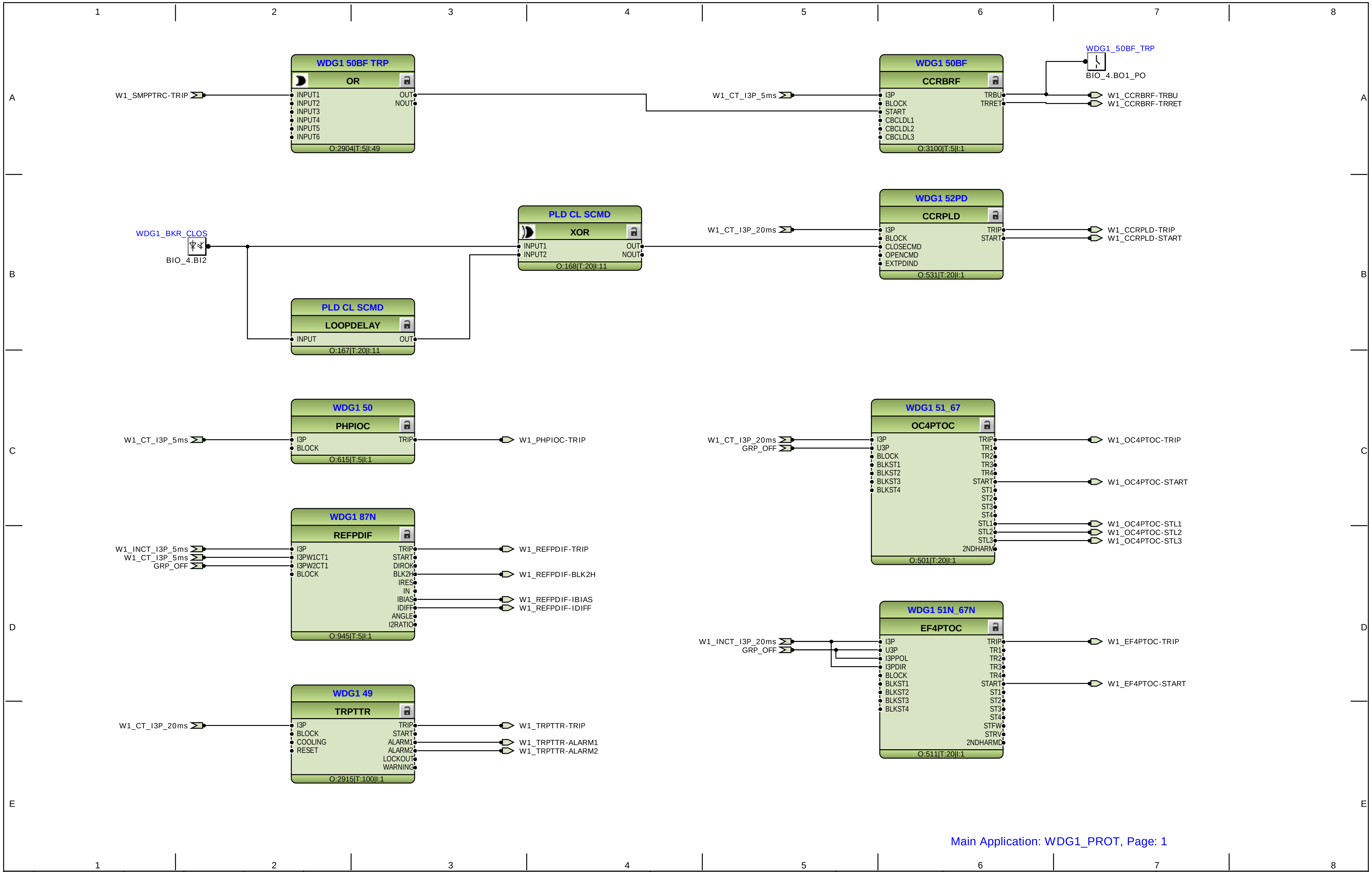
Main Application: INPUTS, Page: 3

					Project Ryerson University	Responsible department ABB Ltd.	Technical reference	Document kind Graphical Application Configuration	Doc. designation AA1J1Q01A3
				Replacing	**Ryerson University** Ryerson University.Substation.Voltage Level.Bay	ABB	Created by	Title RET650	Document id.
Rev.	Modification	Rel. date	Created by	Based on			Approved by		Rev. 0 · Rel. date 6/23/2014 · Lang. en · 6 / 10



Main Application: DIFF_PROT, Page: 1

					Project Ryerson University	Responsible department ABB Ltd.	Technical reference	Document kind Graphical Application Configuration	Doc. designation AA1J1Q01A3
				Replacing	**Ryerson University** Ryerson University.Substation.Voltage Level.Bay	ABB	Created by	Title RET650	Document id.
Rev.	Modification	Rel. date	Created by	Based on			Approved by		Rev. 0 | Rel. date 6/23/2014 | Lang. en



Main Application: WDG1_PROT, Page: 1

Rev. | Modification | Rel. date | Created by | Based on

Replacing

Project
Ryerson University
Ryerson University
Ryerson University.Substation.Voltage Level.Bay

Responsible department
ABB Ltd.

Technical reference

Created by

Approved by

Document kind
Graphical Application Configuration

Title
RET650

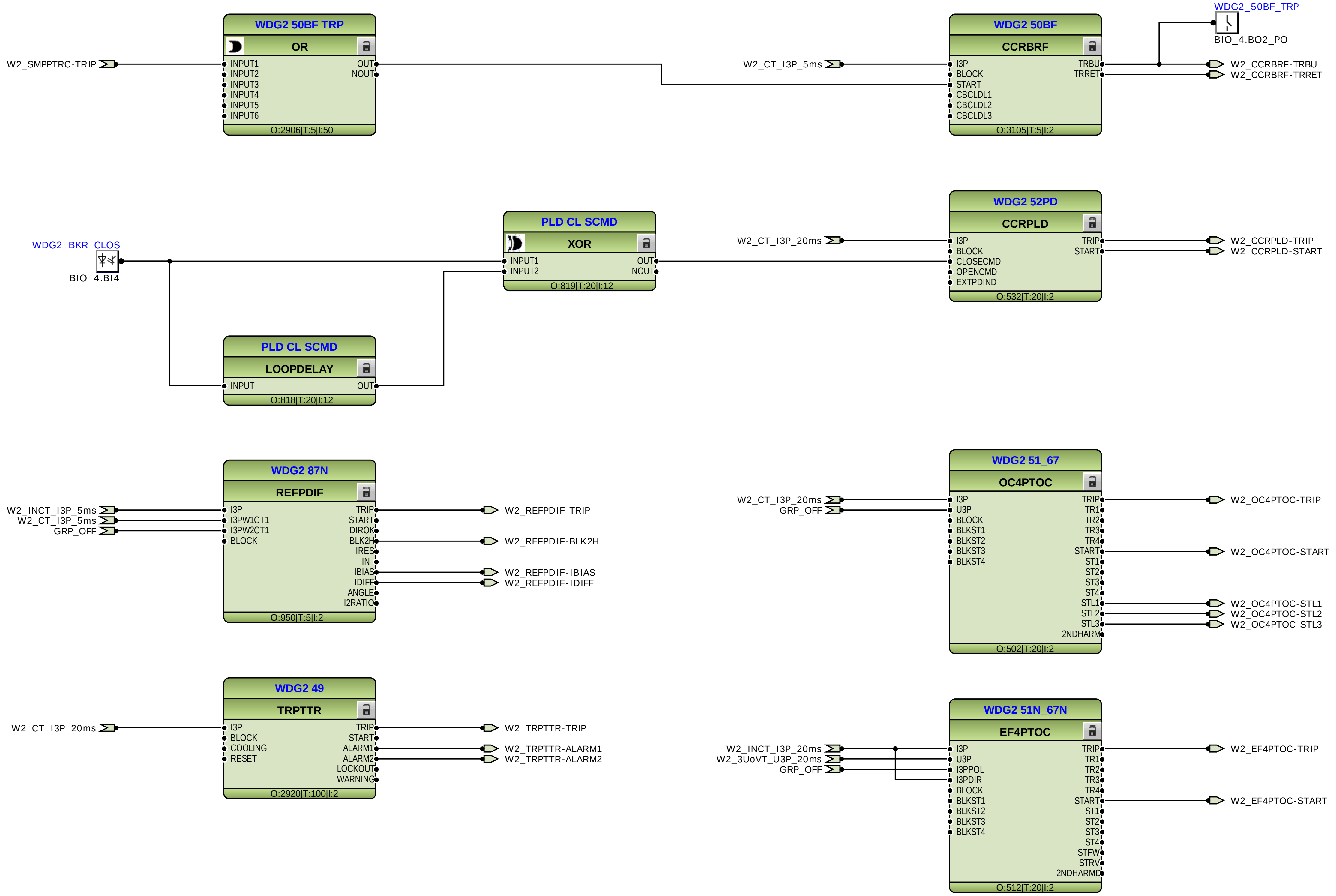
Doc. designation
AA1J1Q01A3

Document id.

Rev.
0

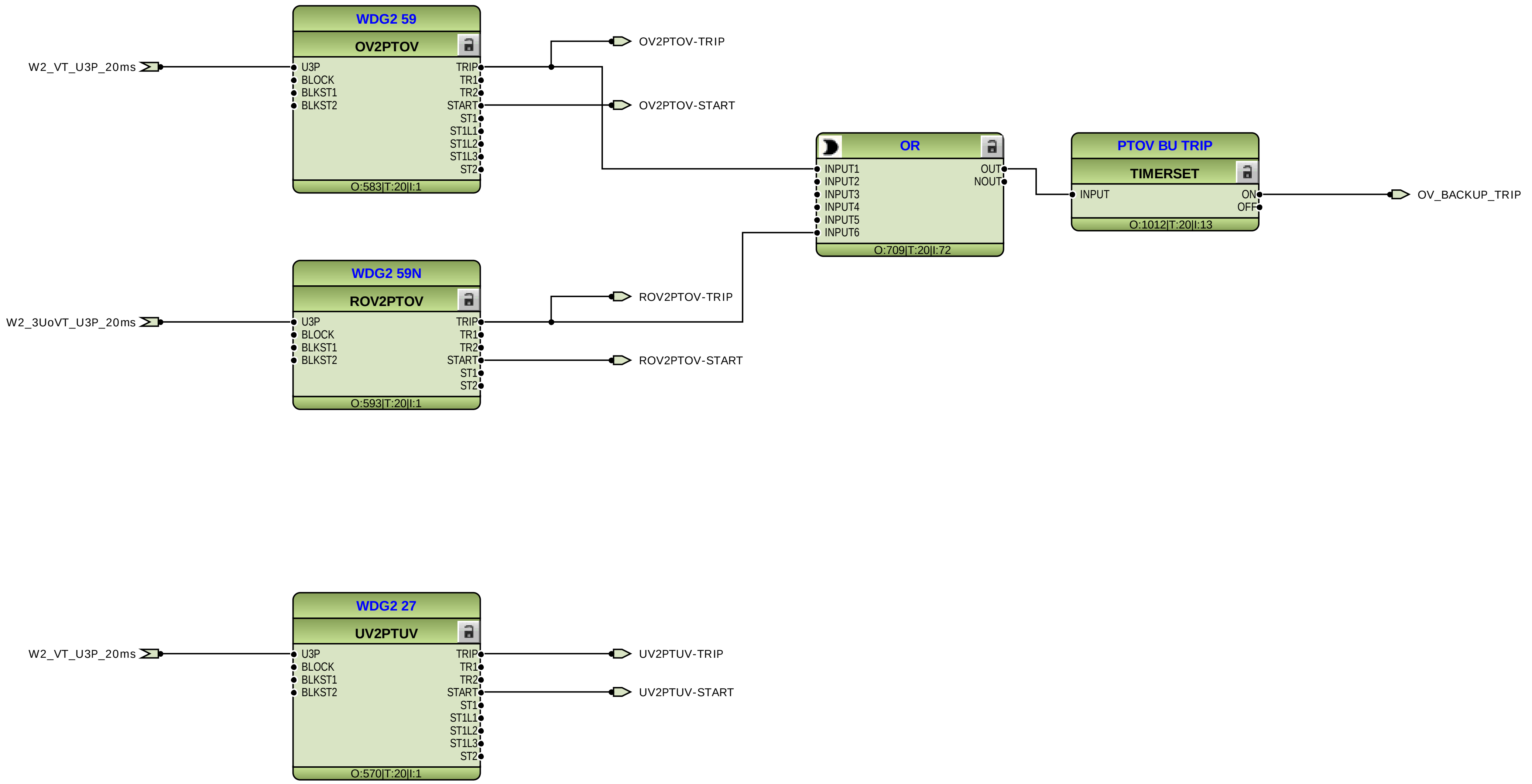
Rel. date
6/23/2014

Lang.
en



Main Application: WDG2_PROT, Page: 1

					Project Ryerson University	Responsible department ABB Ltd.	Technical reference	Document kind Graphical Application Configuration	Doc. designation AA1J1Q01A3
				Replacing	**Ryerson University** Ryerson University.Substation.Voltage Level.Bay		Created by	Title RET650	Document id.
Rev.	Modification	Rel. date	Created by	Based on			Approved by		Rev. 0 / Rel. date 6/23/2014 / Lang. en / 9 / 10



Main Application: WDG2_PROT, Page: 2

Rev.	Modification	Rel. date	Created by	Based on	Replacing

Project
Ryerson University
Ryerson University
Ryerson University.Substation.Voltage Level.Bay

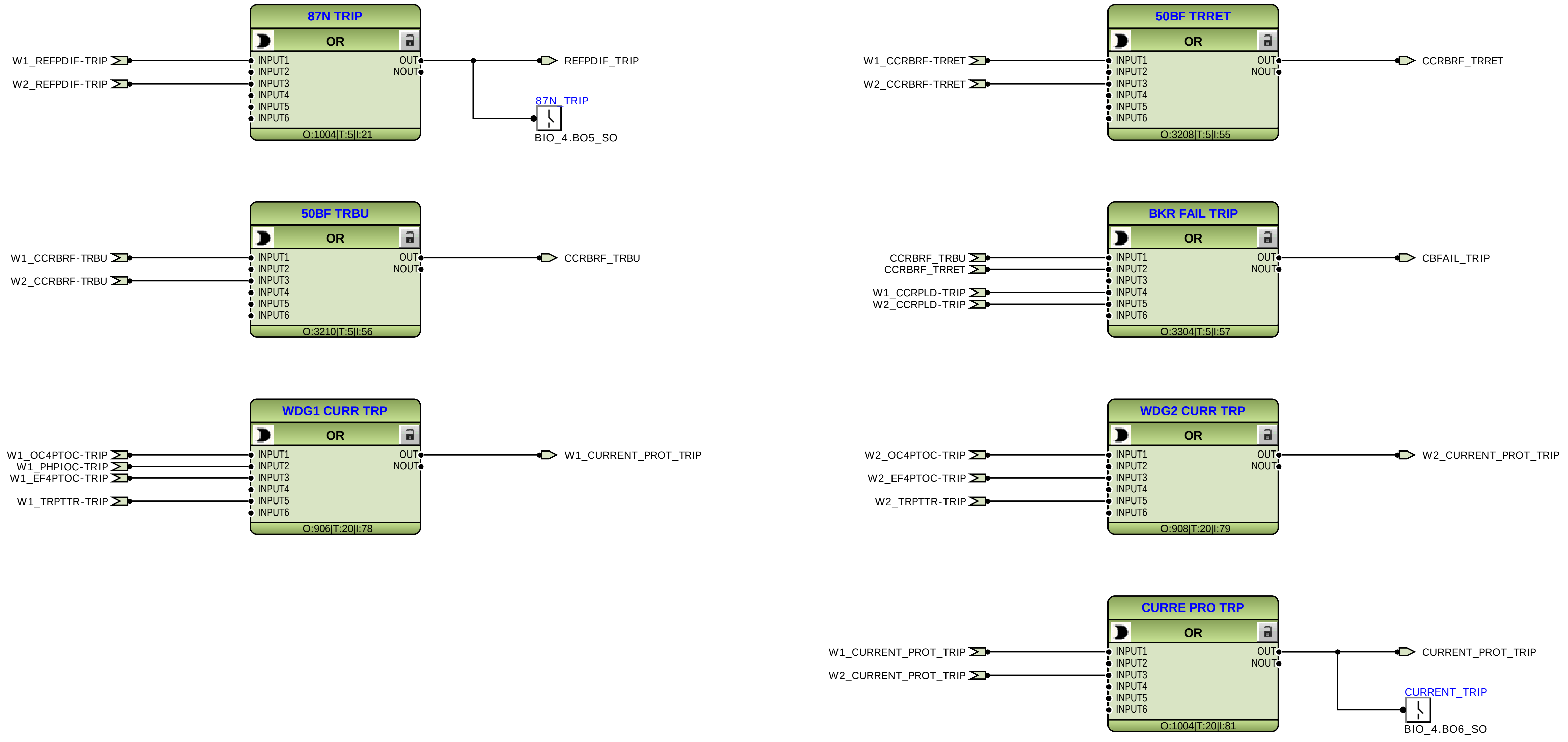
Responsible department
ABB Ltd.

Technical reference
Created by
Approved by

Document kind
Graphical Application Configuration
Title
RET650

Doc. designation
AA1J1Q01A3
Document id.

Rev.	Rel. date	Lang.	
0	6/23/2014	en	10 / 10



Main Application: LOGIC, Page: 1

Rev. | Modification | Rel. date | Created by | Replacing | Based on

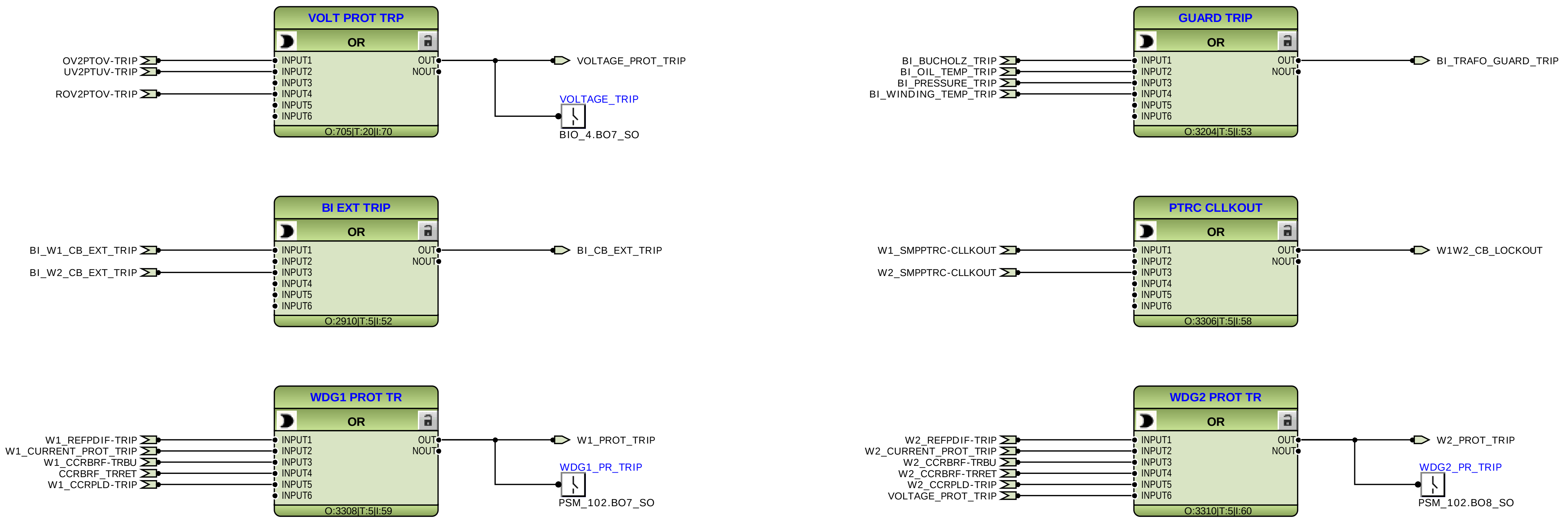
Project
Ryerson University
Ryerson University
Ryerson University.Substation.Voltage Level.Bay

Responsible department
ABB Ltd.

Technical reference
Created by
Approved by

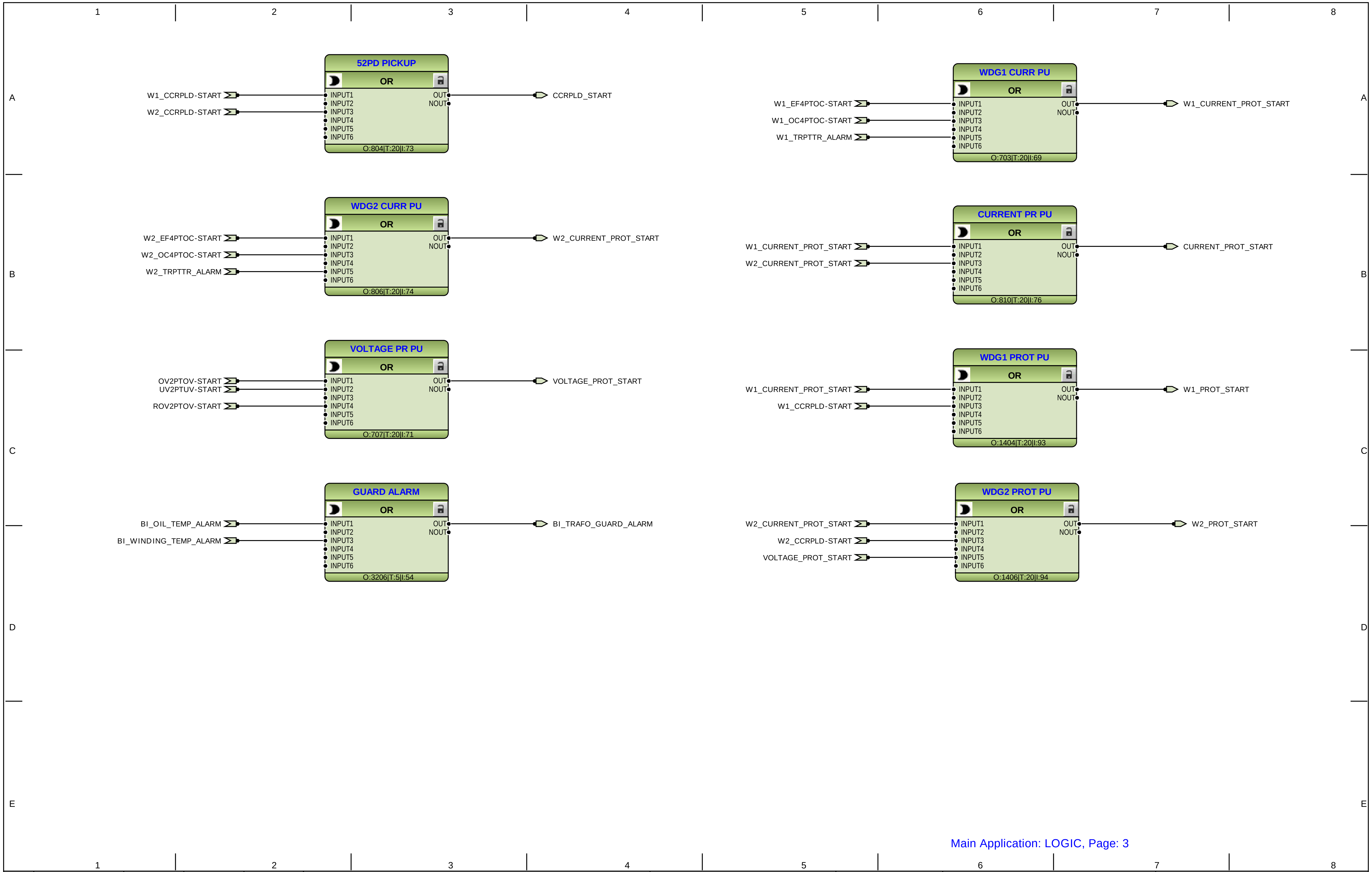
Document kind
Graphical Application Configuration
Title
RET650

Doc. designation
AA1J1Q01A3
Document id.
Rev.
0
Rel. date
6/23/2014
Lang.
en



Main Application: LOGIC, Page: 2

					Project Ryerson University	Responsible department ABB Ltd.	Technical reference	Document kind Graphical Application Configuration	Doc. designation AA1J1Q01A3
				Replacing	**Ryerson University** Ryerson University.Substation.Voltage Level.Bay	ABB	Created by	Title RET650	Document id.
Rev.	Modification	Rel. date	Created by	Based on			Approved by		Rev. 0 Rel. date 6/23/2014 Lang. en 2 / 16



Main Application: LOGIC, Page: 3

Rev. | Modification | Rel. date | Created by | Based on

Replacing

Project
Ryerson University

Ryerson University
Ryerson University.Substation.Voltage Level.Bay

Responsible department
ABB Ltd.

Technical reference

Created by

Approved by

Document kind
Graphical Application Configuration

Title
RET650

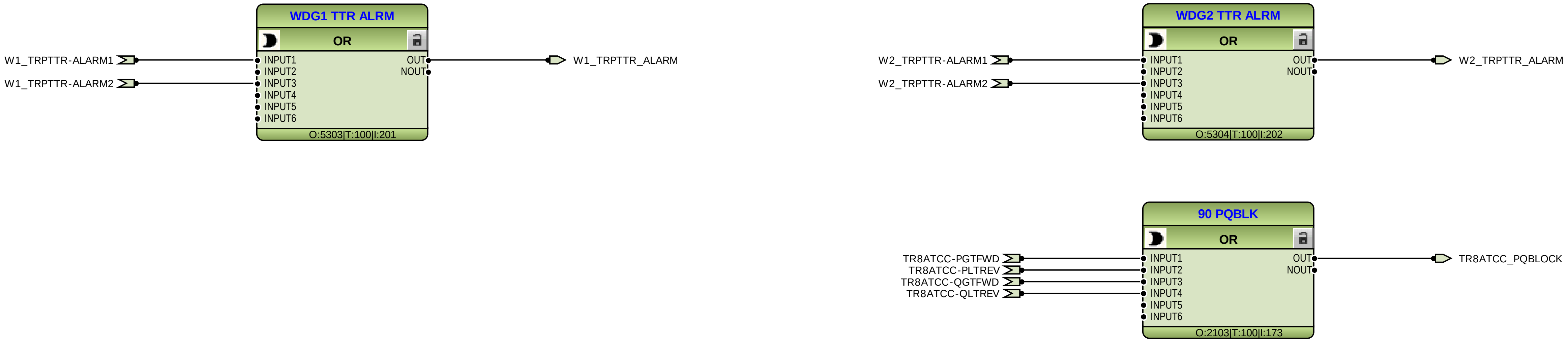
Doc. designation
AA1J1Q01A3

Document id.

Rev.
0

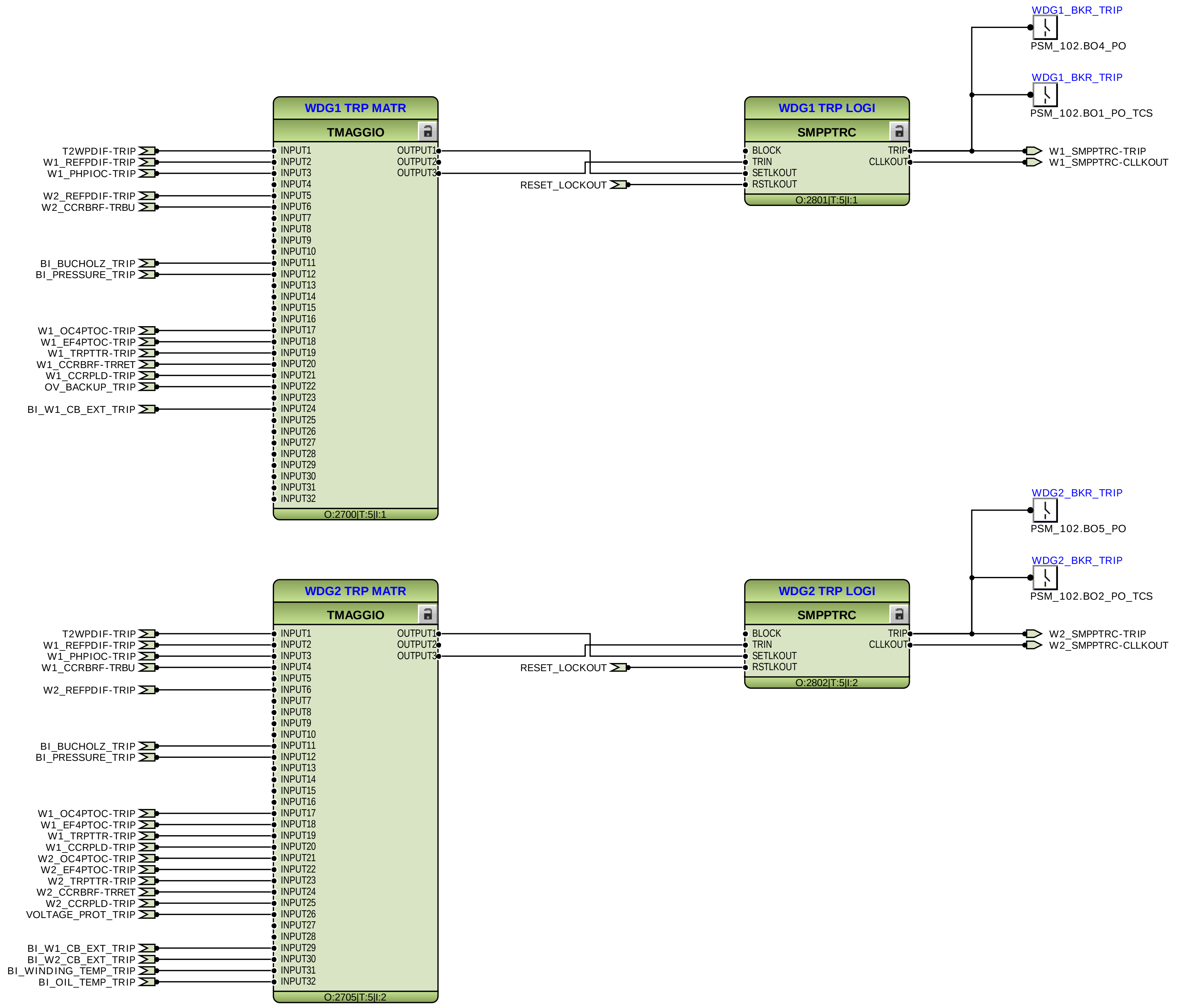
Rel. date
6/23/2014

Lang.
en



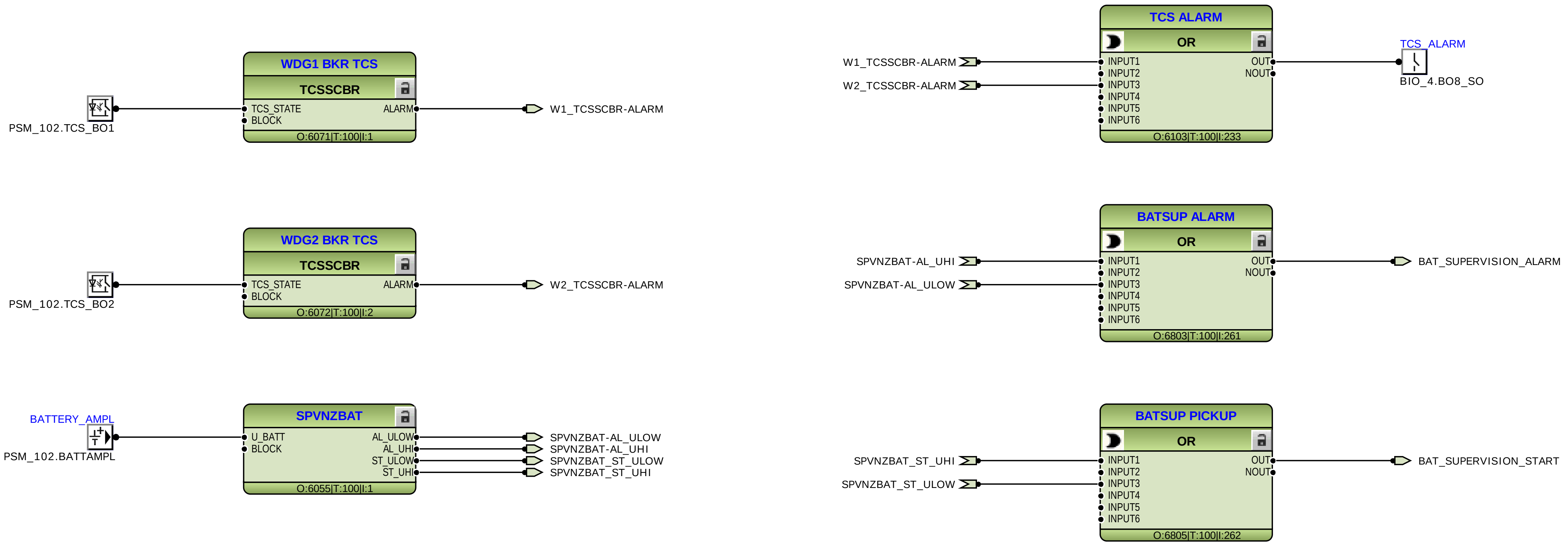
Main Application: LOGIC, Page: 4

Rev.	Modification	Rel. date	Created by	Based on	Replacing	Project	Responsible department	Technical reference	Document kind	Doc. designation
						Ryerson University **Ryerson University** Ryerson University.Substation.Voltage Level.Bay	ABB Ltd. ABB	Created by Approved by	Graphical Application Configuration Title RET650	AA1J1Q01A3 Document id. Rev. 0 Rel. date 6/23/2014 Lang. en



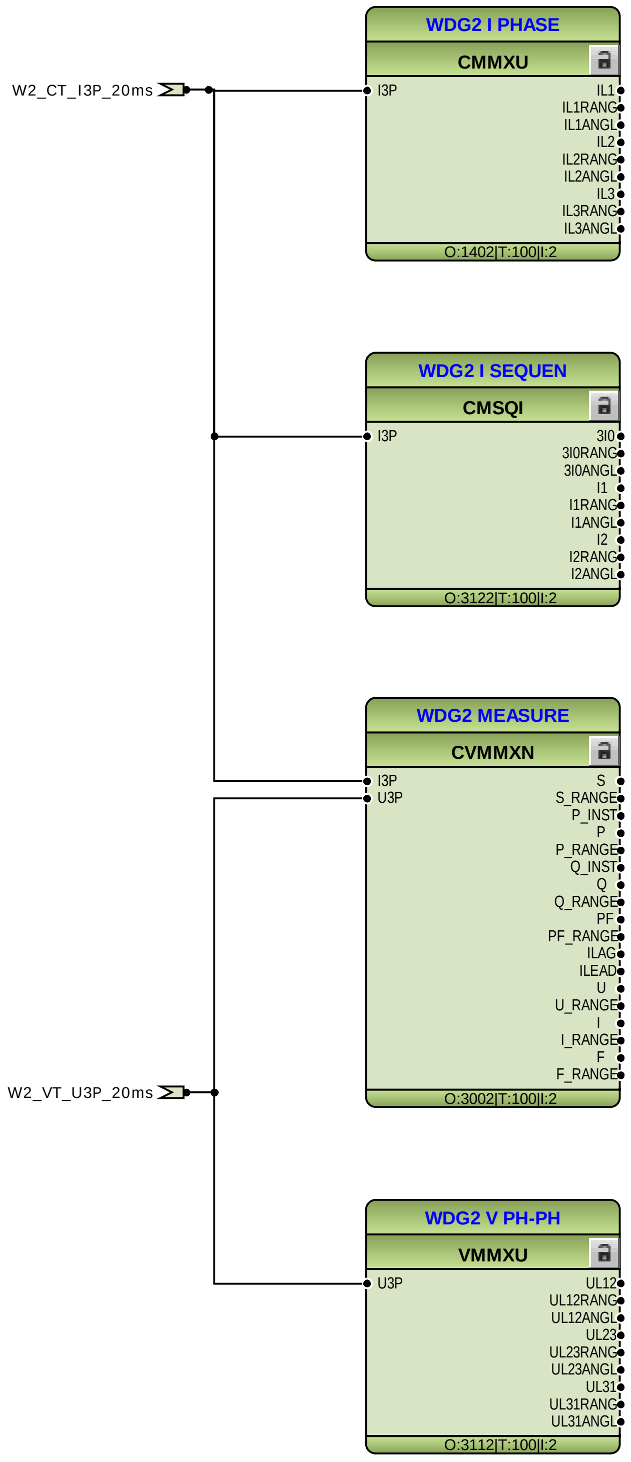
Main Application: TRIP, Page: 1

					Project Ryerson University	Responsible department ABB Ltd.	Technical reference	Document kind Graphical Application Configuration	Doc. designation AA1J1Q01A3
				Replacing	**Ryerson University** Ryerson University.Substation.Voltage Level.Bay		Created by	Title RET650	Document id.
Rev.	Modification	Rel. date	Created by	Based on			Approved by		Rev. 0 Rel. date 6/23/2014 Lang. en 5 / 16



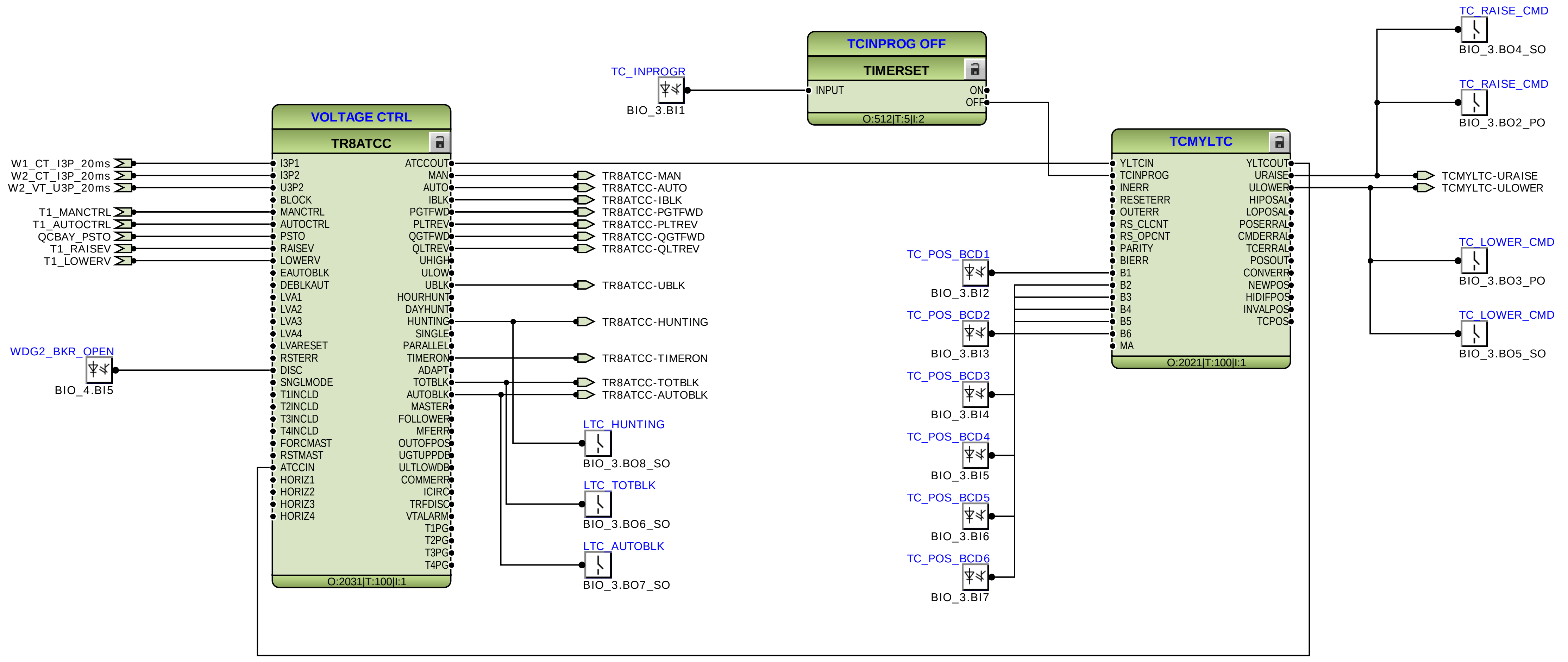
Main Application: COND_MON, Page: 1

					Project Ryerson University	Responsible department ABB Ltd.	Technical reference	Document kind Graphical Application Configuration	Doc. designation AA1J1Q01A3
				Replacing	**Ryerson University** Ryerson University.Substation.Voltage Level.Bay	ABB	Created by	Title RET650	Document id.
Rev.	Modification	Rel. date	Created by	Based on			Approved by		Rev. 0 / Rel. date 6/23/2014 / Lang. en / 6 / 16



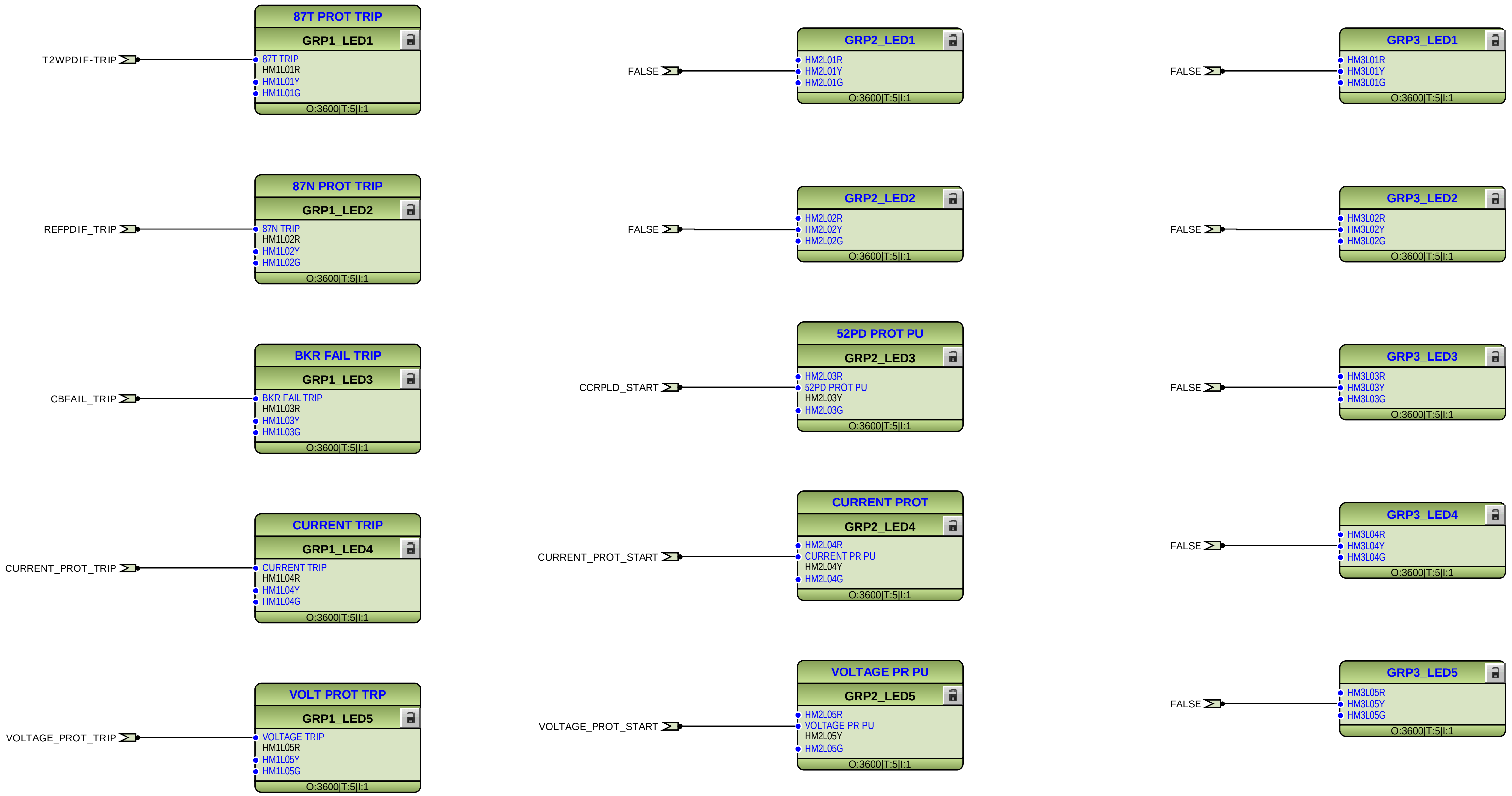
Main Application: MEASURE, Page: 1

					Project Ryerson University	Responsible department ABB Ltd.	Technical reference	Document kind Graphical Application Configuration	Doc. designation AA1J1Q01A3
				Replacing	**Ryerson University** Ryerson University.Substation.Voltage Level.Bay		Created by	Title RET650	Document id.
Rev.	Modification	Rel. date	Created by	Based on			Approved by		Rev. 0 · Rel. date 6/23/2014 · Lang. en



Main Application: VOLTAGE_CONTROL, Page: 1

					Project Ryerson University	Responsible department ABB Ltd.	Technical reference	Document kind Graphical Application Configuration	Doc. designation AA1J1Q01A3
				Replacing	**Ryerson University** Ryerson University.Substation.Voltage Level.Bay		Created by	Title RET650	Document id.
Rev.	Modification	Rel. date	Created by	Based on			Approved by		Rev. 0 Rel. date 6/23/2014 Lang. en 8 / 16



Main Application: OUTPUTS, Page: 1

Project
Ryerson University
Ryerson University
Ryerson University.Substation.Voltage Level.Bay

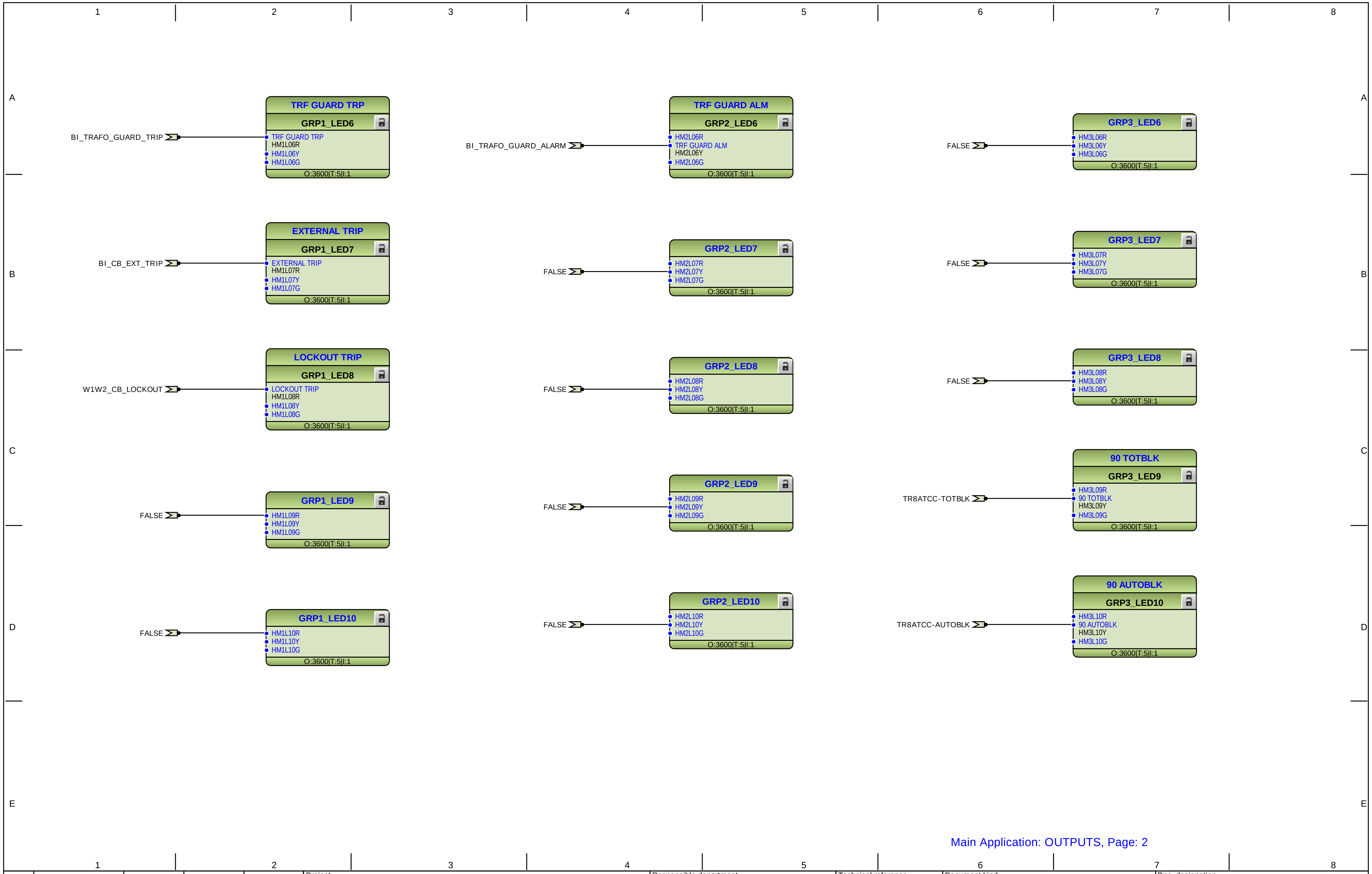
Rev. | Modification | Rel. date | Created by | Replacing | Based on

Responsible department
ABB Ltd.

Technical reference
Created by
Approved by

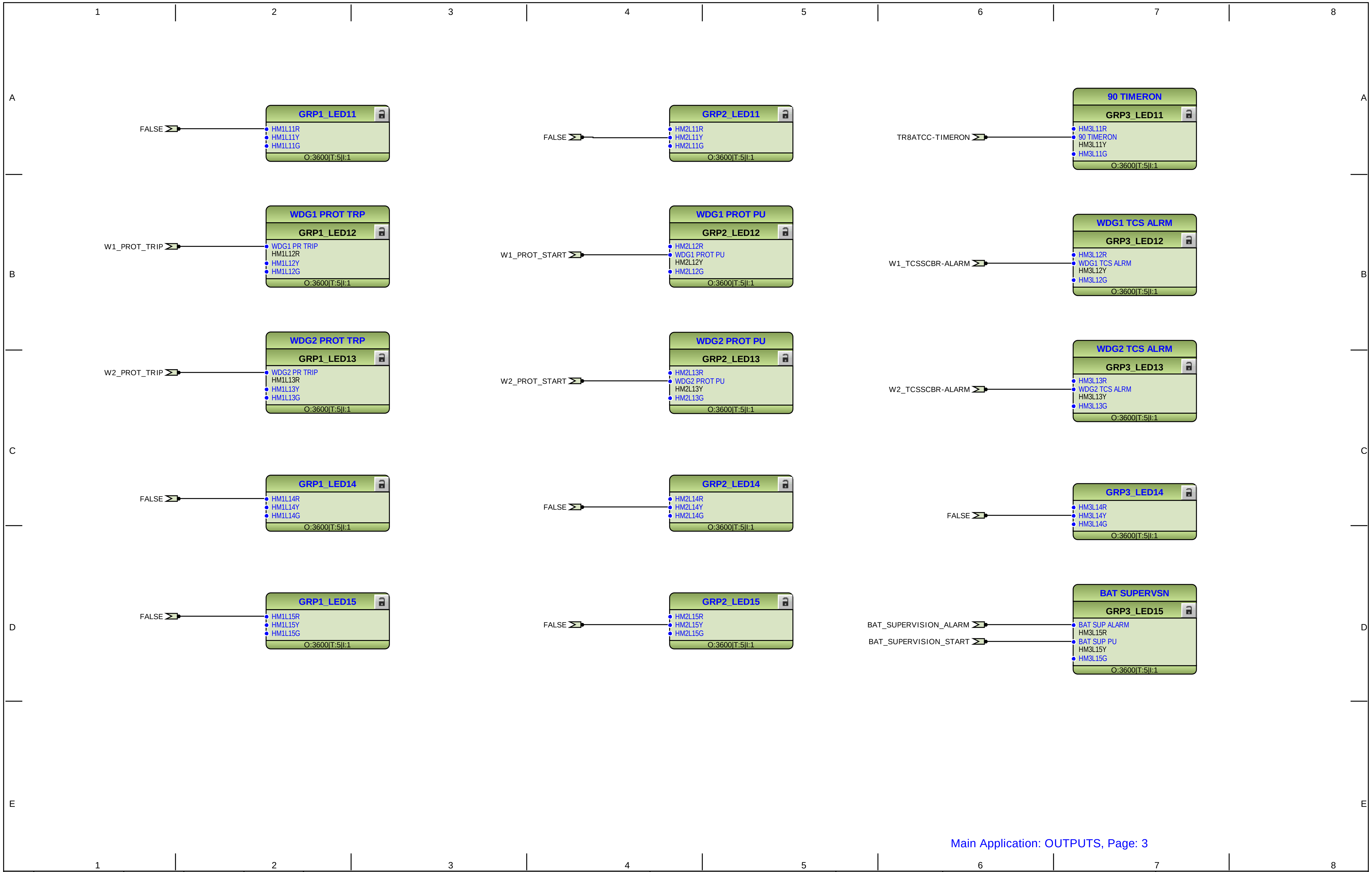
Document kind
Graphical Application Configuration
Title
RET650

Doc. designation
AA1J1Q01A3
Document id.
Rev. 0
Rel. date 6/23/2014
Lang. en



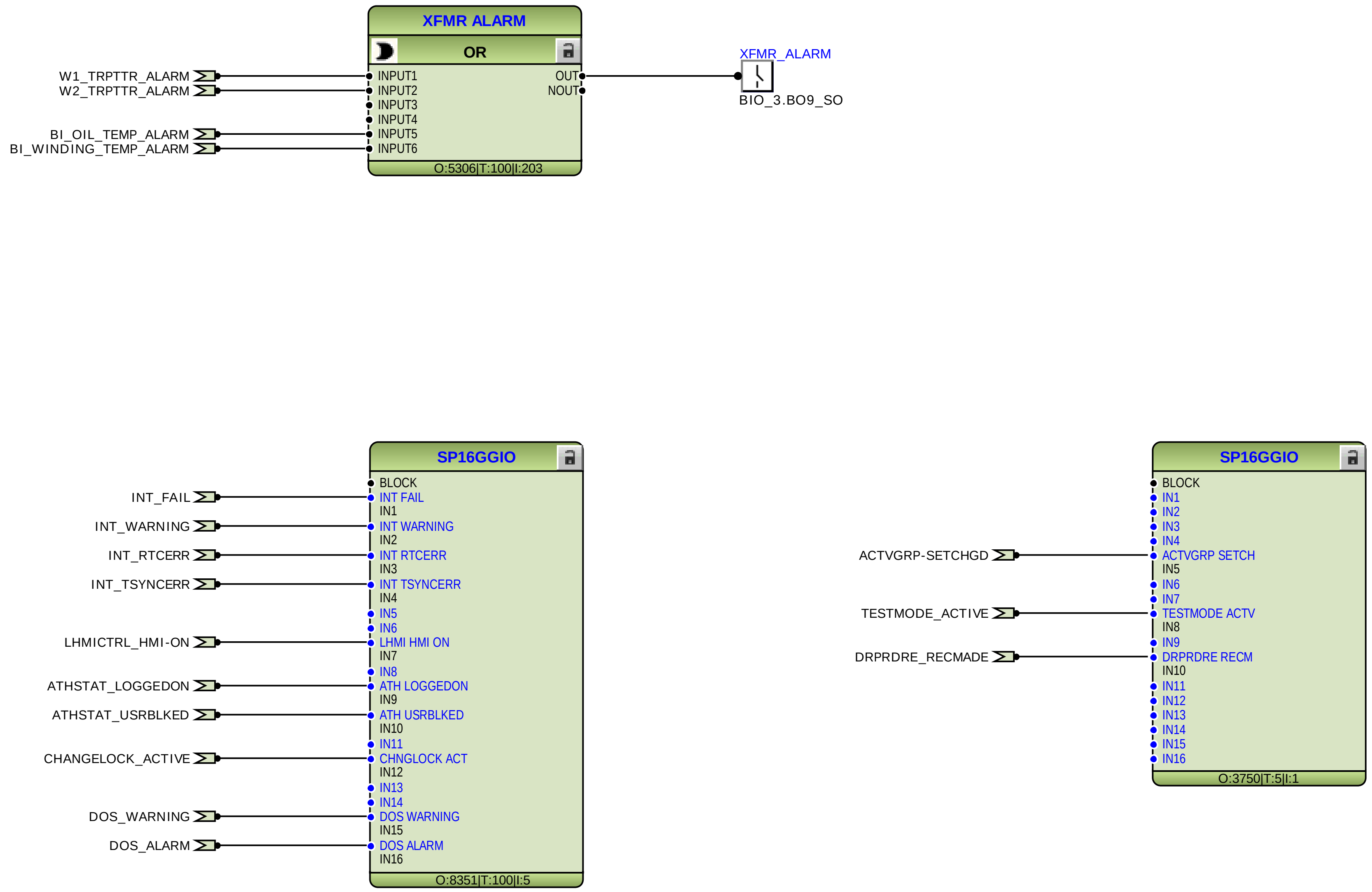
Main Application: OUTPUTS, Page: 2

					Project Ryerson University	Responsible department ABB Ltd.	Technical reference	Document kind Graphical Application Configuration	Doc. designation AA1J1Q01A3
				Replacing	**Ryerson University** Ryerson University.Substation.Voltage Level.Bay	ABB	Created by	Title RET650	Document id.
Rev.	Modification	Rel. date	Created by	Based on			Approved by		Rev. 0 | Rel. date 6/23/2014 | Lang. en | 10 / 16



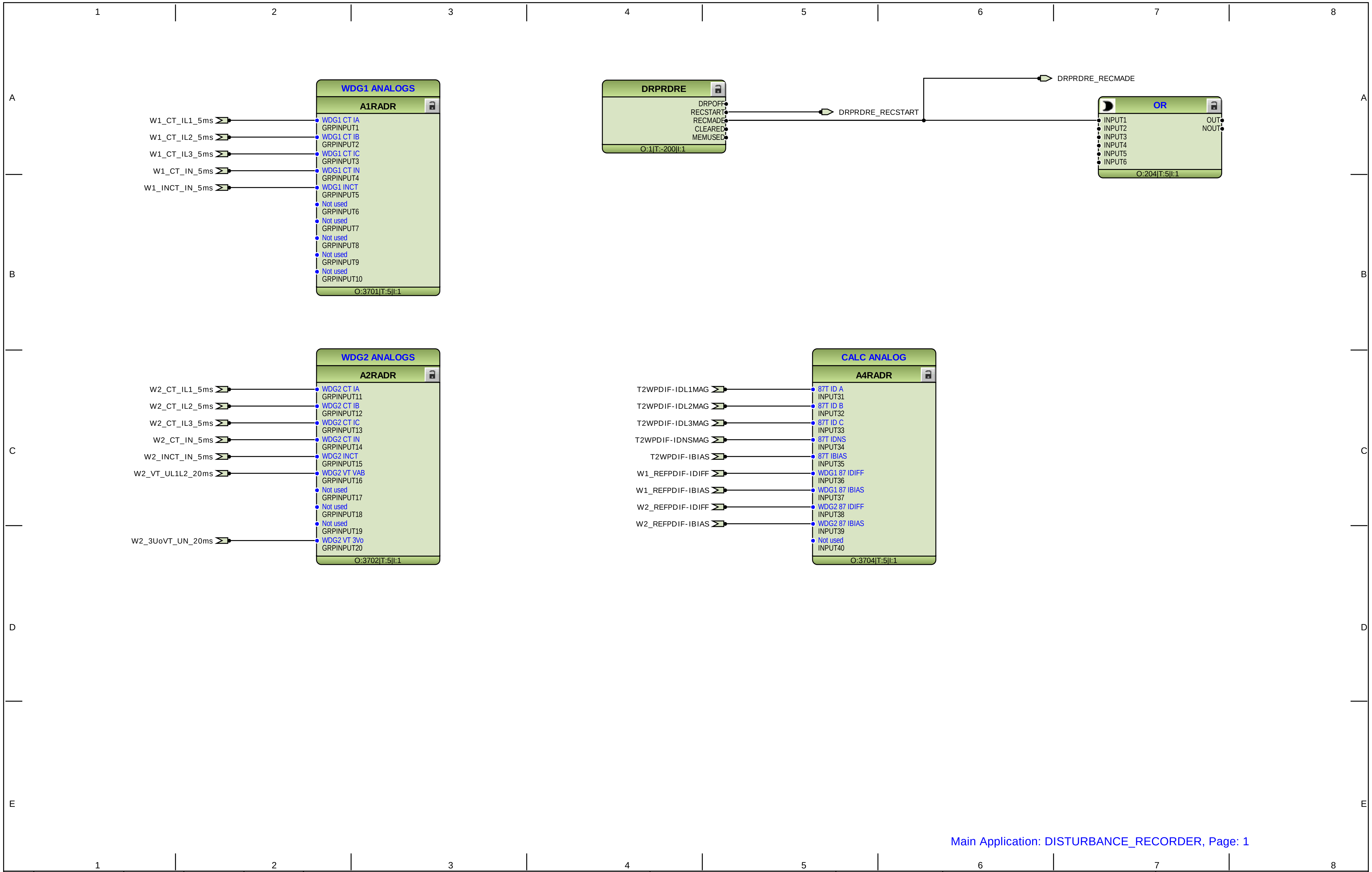
Main Application: OUTPUTS, Page: 3

Rev.	Modification	Rel. date	Created by	Replacing Based on	Project	Responsible department	Technical reference	Document kind	Doc. designation
					Ryerson University	ABB Ltd.		Graphical Application Configuration	AA1J1Q01A3
					Ryerson University Ryerson University.Substation.Voltage Level.Bay		Created by Approved by	Title RET650	Document id. Rev. 0 Rel. date 6/23/2014 Lang. en



Main Application: OUTPUTS, Page: 4

					Project Ryerson University	Responsible department ABB Ltd.	Technical reference	Document kind Graphical Application Configuration	Doc. designation AA1J1Q01A3			
				Replacing	**Ryerson University** Ryerson University.Substation.Voltage Level.Bay		Created by	Title RET650	Document id.			
Rev.	Modification	Rel. date	Created by	Based on			Approved by		Rev. 0	Rel. date 6/23/2014	Lang. en	12 / 16



Main Application: DISTURBANCE_RECORDER, Page: 1

Rev.	Modification	Rel. date	Created by	Based on
				Replacing

Project
Ryerson University
Ryerson University
Ryerson University.Substation.Voltage Level.Bay

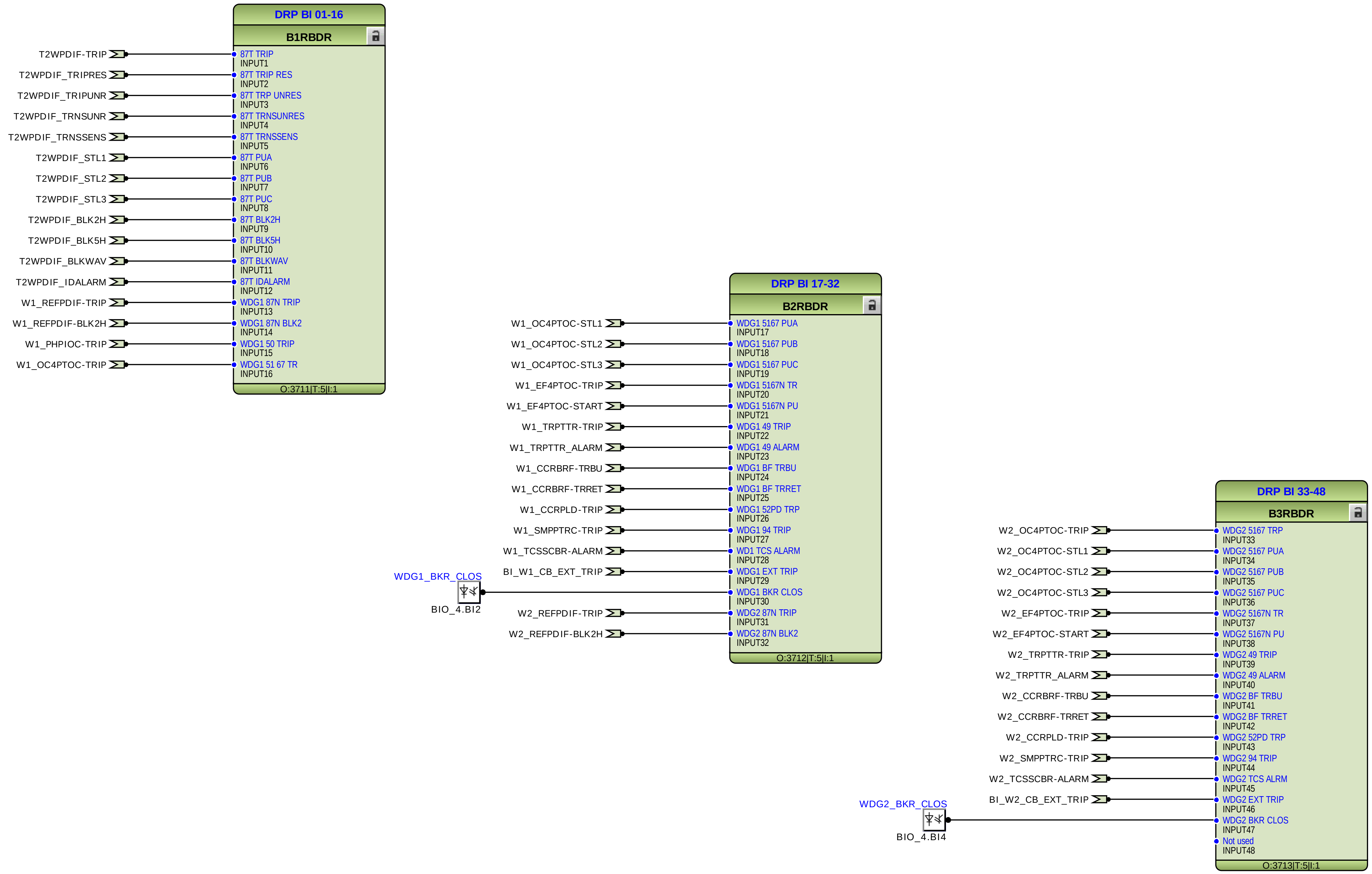
Responsible department
ABB Ltd.

Technical reference
Created by
Approved by

Document kind
Graphical Application Configuration
Title
RET650

Doc. designation
AA1J1Q01A3
Document id.

Rev.	Rel. date	Lang.	
0	6/23/2014	en	13 / 16



Main Application: DISTURBANCE_RECORDER, Page: 2

Rev.	Modification	Rel. date	Created by	Based on	Replacing

Project
Ryerson University
Ryerson University
Ryerson University.Substation.Voltage Level.Bay

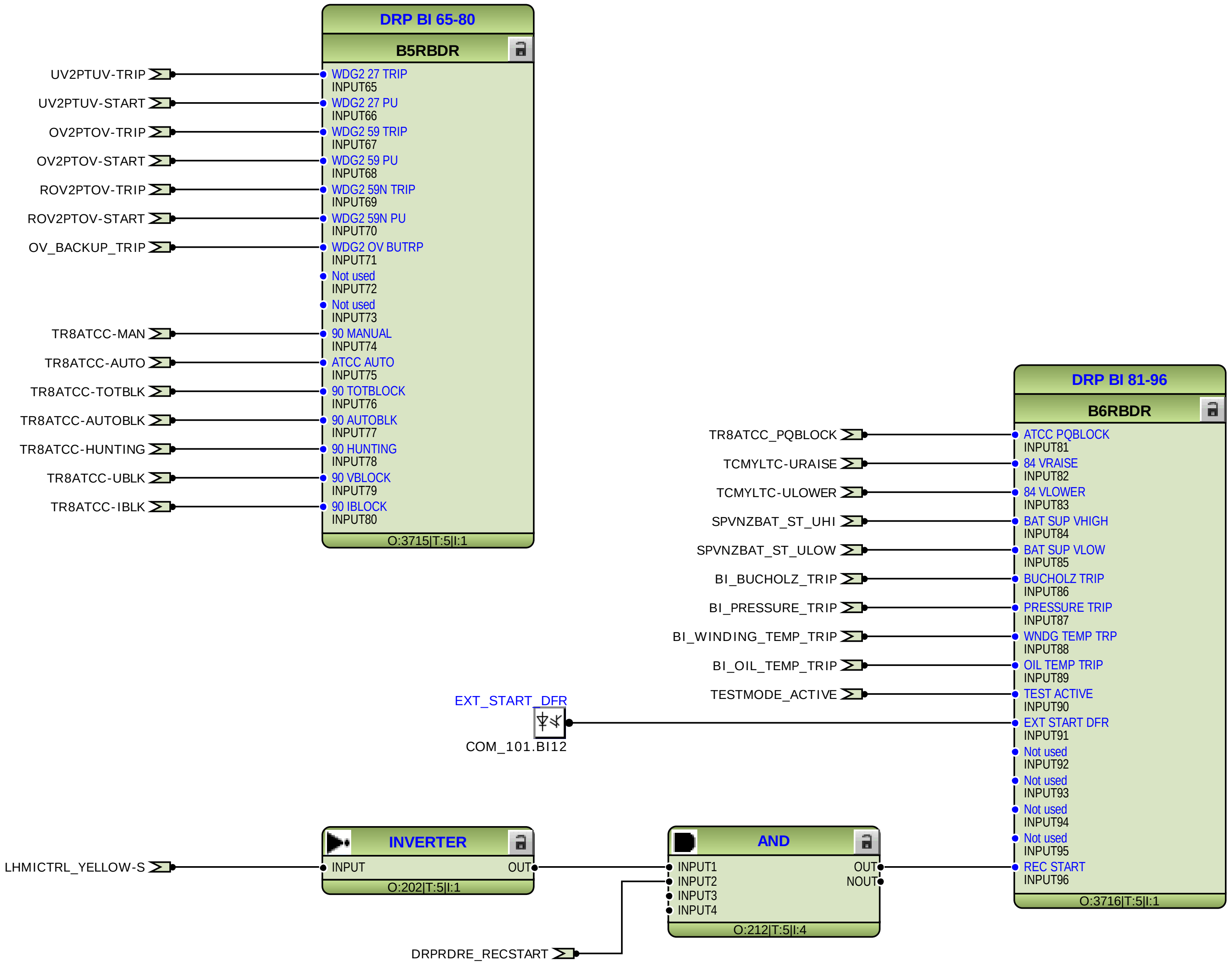
Responsible department
ABB Ltd.

Technical reference
Created by
Approved by

Document kind
Graphical Application Configuration
Title
RET650

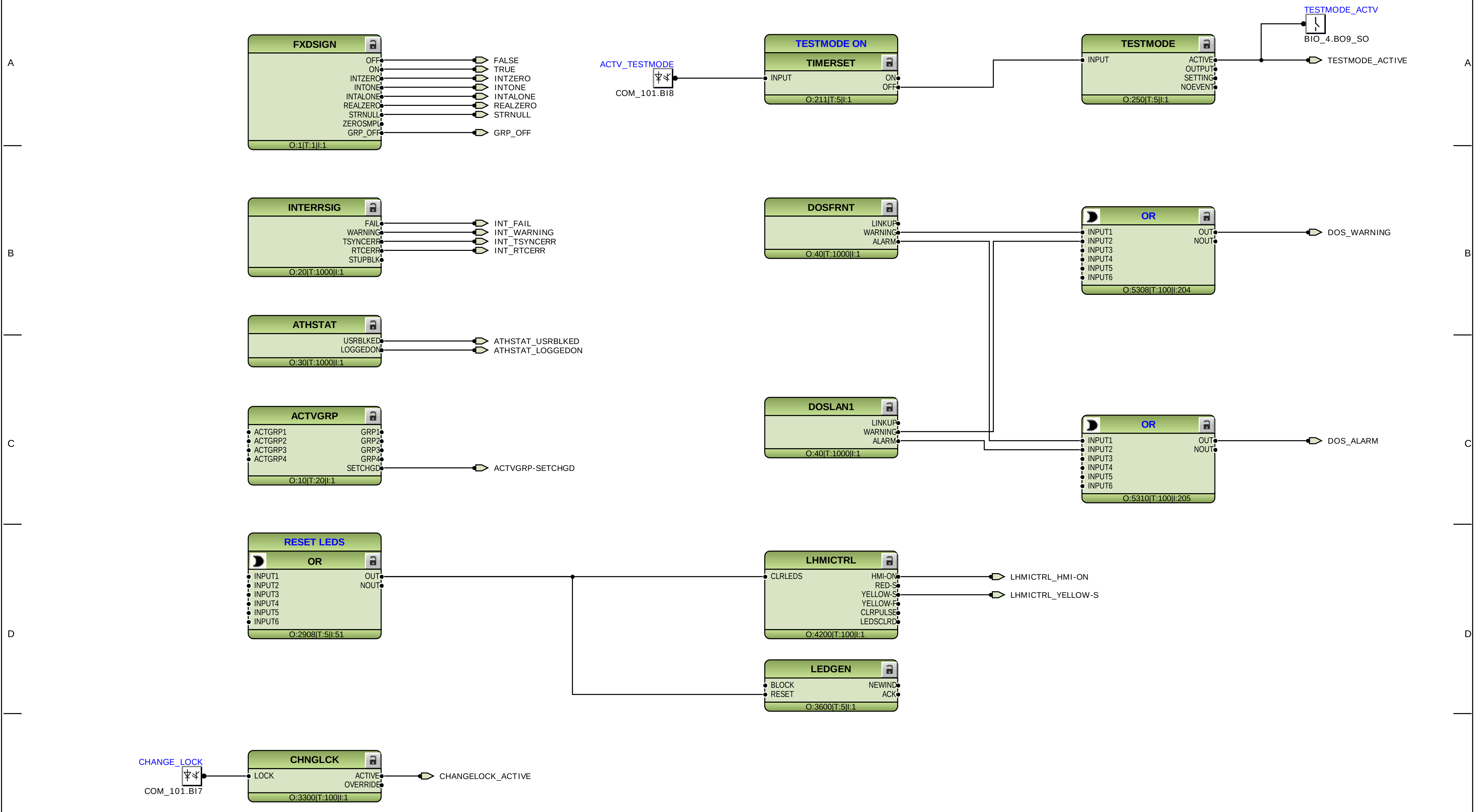
Doc. designation
AA1J1Q01A3
Document id.

Rev.	Rel. date	Lang.	
0	6/23/2014	en	



Main Application: DISTURBANCE_RECORDER, Page: 3

					Project Ryerson University	Responsible department ABB Ltd.	Technical reference	Document kind Graphical Application Configuration	Doc. designation AA1J1Q01A3			
				Replacing	**Ryerson University** Ryerson University.Substation.Voltage Level.Bay	ABB	Created by	Title RET650	Document id.			
Rev.	Modification	Rel. date	Created by	Based on			Approved by		Rev. 0	Rel. date 6/23/2014	Lang. en	15 / 16



Main Application: COMMON, Page: 1

					Project Ryerson University	Responsible department ABB Ltd.	Technical reference	Document kind Graphical Application Configuration	Doc. designation AA1J1Q01A3
				Replacing	**Ryerson University** Ryerson University.Substation.Voltage Level.Bay	ABB	Created by	Title RET650	Document id.
Rev.	Modification	Rel. date	Created by	Based on			Approved by		Rev. 0 / Rel. date 6/23/2014 / Lang. en / 16 / 16

References

[1] NETL Project M63SNL34 “Cyber Security for Utility Operations” Final report of this project is available from DoE Office of Energy Assurance or from Sandia National Laboratories

[2] “Model-Based Attack Detection and Mitigation for AGC” by Siddharth Sridhar and Manimaran, IEEE Transaction March 2014

[3] AGA 12 Part 1 “Cryptographic Protection of SCADA Communications Part 1 Background, Policies and Test Plan” available from Gas Technology Institute

[4] “Securing Telecontrol in Smart Grid Environments” by Steffen Fries and Andre Suhr Siemens Germany, International ETG Kongress 2013

[5] PSRC C3 Processes, Issues, Trends and Quality Control of Relay Settings

[6] Pilot Protection Communications Channel Requirement, S. Ward et. al., Georgia Tech,

[7] Electronic Security of Real-Time Protection and SCADA Communications. Allen Risley, et al. Schweitzer Engineering Laboratories, Inc. WPDAC

[8] Integrated Anomaly Detection for Cyber Security of the Substations” by Junho Hong, Chen-Ching, Manimaran, IEEE transaction July 2014

[9] Shea, Dana, “Critical Infrastructure: Control Systems and the Terrorist Threat” Report For Congress, Order Code RL31534

[10] IEC TC57 WG15 Security Standards – White paper by Xanthus Consulting International

[11] NERC – Security Guidelines for the Electricity Sector: Securing Remote Access to Electronic Control and Protection Systems.

[12] Role Based Access, a proposed standard for RBAC prepared by NIST, available at http://csrc.nist.gov/rbac/

[13] SE Linux software, documentation, and related publications are available for download from the NSA web site (http://www.nsa.gov/selinux/)

[14]“Cyber Security Requirements and Related Standards for Substation Automation Systems” by F. Hohlbaum, P.Schwyter, F. Alvarez

[15]“Cyber Security Practical Considerations for Implementing IEC62351” by Frank, Markus Braendle

[16]“Sorting Out NERC, NIST and DOE” by David Dolezilek, Laura Hussey

[17]“The Design of Information Security Protection Framework to Support Smart Grid” by Tao Zhang, Weimin Lin, YufeiWang

[18]“Technical Reference Manual IED RET650650” by ABB Sweden

[19]“Cyber Attacks, Countermeasures and Challenges” by Xu Li, Haojin Zhu, Xiaohui Liang

[20]“A Conceptual Framework for Smart Grid” by Chengbing Wei

[21]“Protection and Control IED RET650 Manager” by ABB Switzerland

[22]“Developing Cyber Physical Experimental Capabilities for Security Analysis of the Future Smart Grid” by Bela Genge, Christos Siaterlis

[23]“Protecting Smart Grid Automation Systems Against Cyberattacks” by Dong Wie, Yan Lu

[24]“A Survey on Cyber Security for Smart Grid Communication” by Ye Yan, Yi Qian, Hamid Sharif, David Tipper

[25]“Securing Telecontrol in Smart Grid Environment” by Steffen Fries, Andre Suhr, ETG Kongress 2013

[26]“Encryption Key Management for Secure Communication in Smart Advanced Metering Infrastructure” by Seung Hyun, Xiaoyu and Elisa, IEEE Smart Grid Communication 2013 Symposium.

[27]“Fault Detection with Discrete-Time Measurements” by Erasmia Evangelia, Peyman and John, IEEE Conference on Decision and Control December 2013.

[29]“Bio-Inspired Cyber Security for Smart Grid Deployment” by David, Seth, Ruslan, IEEE Transaction 2013.

[30]S.-M. Amin and A. M. Giacomoni, “Smart grid- safe, secure, selfhealing: Challenges and opportunities in power system security, resiliency, and privacy,” IEEE Power EnergyMag., pp. 33–40, Jan. 2012.

[31]G. Dan, H. Sandberg, M. Ekstedt, and G. Bjorkman, “Challenges in power system information security,” IEEE Security Privacy, vol. 10, no. 4, pp. 62–70, Jul. 2012.

[32]D. Kushner, “The real story of Stuxnet,” IEEE Spectrum, vol. 50, no. 3, pp. 48–53, Mar. 2013.

[33]S. Sridhar, A. Hahn, and M. Govindarasu, “Cyber-physical system security for the electric power grid,” Proc. IEEE, vol. 100, no. 1, pp. 210–224, Jan. 2012.

[34]M. Govindarasu, A. Hann, and P. Sauer, “Cyber-physical systems security for smart grid,” Future Grid Initiative White Paper, PSERC, Feb. 2012

[35]M. Esmalifalak, G. Shi, Z. Han, and L. Song, “Bad data injection attack and defense in electricity market using game theory study,” IEEE Trans. Smart Grid, vol. PP, no. 99, pp. 1–10, 2013.

[36] NERC CIP- Cyber Security Regulations for North American Power Utilities- Critical Infrastructure Protection.

[37] IEC62351- Data and Communication Security.

[38] IEEE PSRC H13- Cyber Security Requirements for Substation Automation, Protection and Control Systems.

[39] IEEE1686- IEEE Standard for Substation Intelligent Electronic Devices Cyber Security Capabilities.