CYBER SECURITY

CHAPTER 18

Date	06/2014
Hardware Suffix:	L and later
Software Version:	B1

CONTENTS

TABLES

FIGURES

Page (CS) 18-

Notes:

1 OVERVIEW

1.1 History

In the past, substation networks were traditionally isolated and the protocols and data formats used to transfer information between Intelligent Electronic Devices (IEDs) were often proprietary.

For these reasons, isolated substation environments were very secure against cyber attacks. The terms used for this inherent type of security are:

- Security by isolation (if the substation network is not connected to the outside world, it can't be accessed from the outside world).
- Security by obscurity (if the formats and protocols are proprietary, it is very difficult, to interpret them.

The introduction of Cyber Security tools has resulted in many new terms. You can see a list of some of these in the Glossary for Cyber Security section.

1.2 Lone and Connected Grids

For many years protection equipment (such as relays or IEDs) would often be used to protect a lone network. By "lone" we mean one IED would protect one network; with only a very restricted opportunity for the device to communicate with the outside network. This would be because of a lack of internet access to the network or the IED; and connections being largely at the IED itself. Access to these systems was often possible because some-one logged on to the IED using a password; which granted them a range of pre-set access levels. Such access was traditionally done by using the buttons on the front panel on the IED; or by connecting a computer to the IED using a short cable.

The increasing sophistication of protection schemes coupled with the advancement of technology and the desire for vendor interoperability has resulted in standardization of networks and data interchange within substations. Today, most devices within substations generally use standardized protocols for communication.

Over time, systems have become more connected; with open and/or internet connectivity and the ability to access IEDs from computers connected directly to the IED or remotely (from internet-based or corporate-wide networks). Threats such as hacking, malware, worms and viruses; and the use of common operating systems (such as Windows and Linux) has increased the vulnerability of computer systems. Because these systems are more connected, there is now a major security risk making the grid vulnerable to cyber-attacks or unauthorized access, which could in turn lead to major electrical outages.

An illustration of Lone Grids is shown in Figure 1 and Connected Grids Figure 2.

To mitigate these risks, cyber security features have been introduced on devices, such as IEDs and computers. In the context of IEDs, this will include things such as equipment hardening and enhanced access restrictions. In the context of computer systems, this will include firewalls, data encryption and various protection software. These are intended to secure communications and equipment within substation environments. This chapter describes the security measures that have been put in place for Schneider Electric's MiCOM P40 range of IEDs.

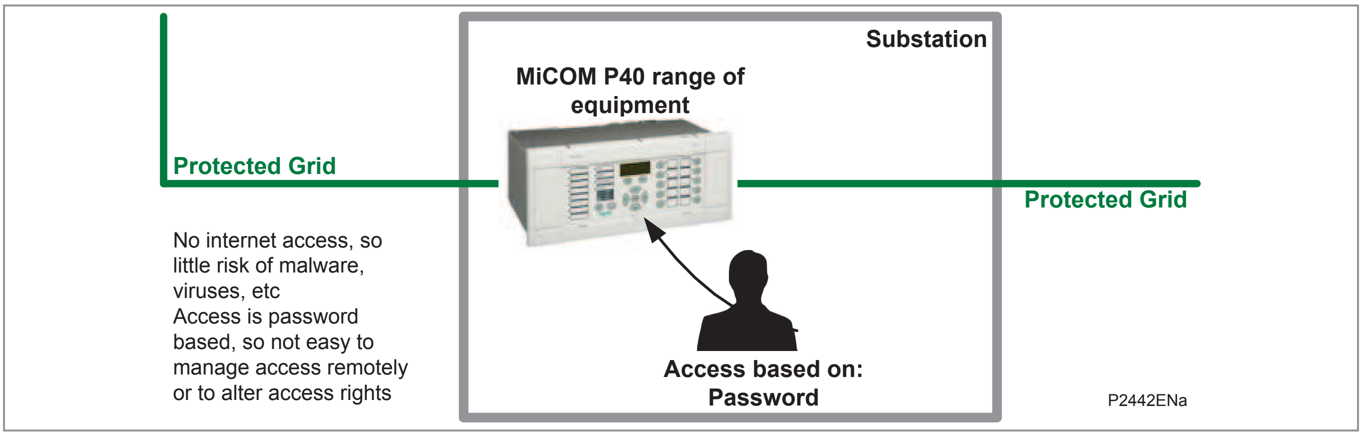
Substation
MiCOM P40 range of equipment
Protected Grid
Protected Grid
No internet access, so little risk of malware, viruses, etc
Access is password based, so not easy to manage access remotely or to alter access rights
Access based on: Password
P2442ENa

Figure 1 - Lone Grids

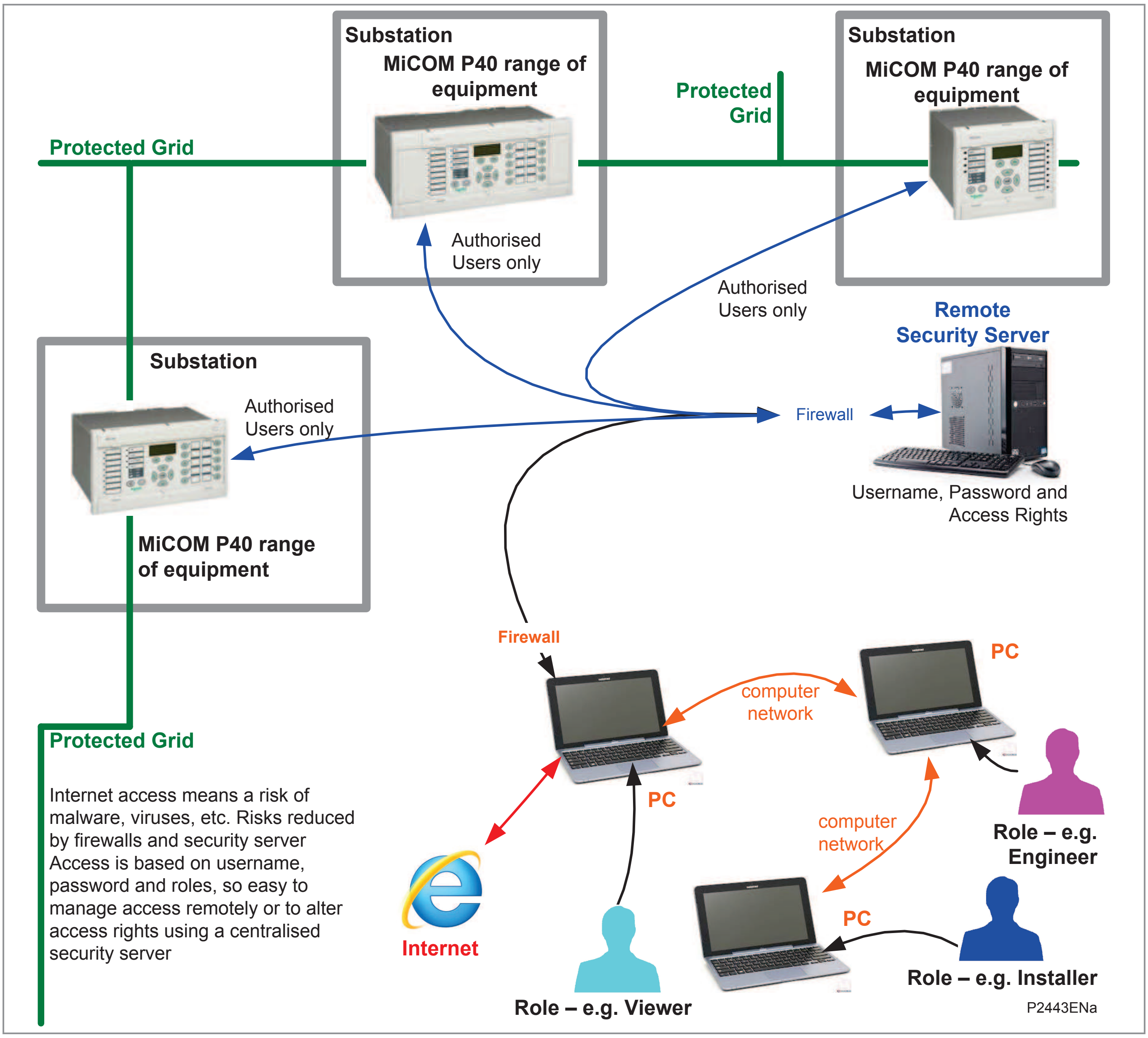
Substation
MiCOM P40 range of equipment
Substation
MiCOM P40 range of equipment
Protected Grid
Protected Grid
Authorised Users only
Authorised Users only
Remote Security Server
Substation
Authorised Users only
Firewall
Username, Password and Access Rights
MiCOM P40 range of equipment
Firewall
PC
computer network
Protected Grid
PC
computer network
Role – e.g. Engineer
Internet access means a risk of malware, viruses, etc. Risks reduced by firewalls and security server
Access is based on username, password and roles, so easy to manage access remotely or to alter access rights using a centralised security server
PC
Internet
Role – e.g. Installer
Role – e.g. Viewer
P2443ENa

Figure 2 - Connected Grids

1.3 Cyber Security Protection

Cyber security provides protection against unauthorized disclosure, transfer, modification, or destruction of information and/or information systems, whether accidental or intentional. To achieve this, there are several security requirements:

- Confidentiality (preventing unauthorized access to information)
- Integrity (preventing unauthorized modification)
- Availability / Authentication (preventing the denial of service and assuring authorized access to information)
- Non-Repudiation (preventing the denial of an action that took place)
- Traceability/Detection (monitoring and logging of activity to detect intrusion and analyze incidents)

The threats to cyber security may be unintentional (e.g. natural disasters, human error), or intentional (e.g. cyber attacks by hackers).

Good cyber security can be achieved with a range of measures, such as closing down vulnerability loopholes, implementing adequate security processes and procedures and providing technology to help achieve this.

Examples of vulnerabilities are:

- Indiscretions by personnel (e.g. users keep passwords on their computer)
- Bypassing of controls (e.g. users turn off security measures)
- Bad practice (users do not change default passwords, or everyone uses the same password to access all substation equipment)
- Inadequate technology (e.g. substation is not firewalled)

Examples of availability issues are:

- Equipment overload, resulting in reduced or no performance
- Expiry of a certificate prevents access to equipment.

To help tackle these issues, standards organizations have produced various standards, by which compliance significantly reduces the threats associated with lack of cyber security. These standards are described in more detail in the Standards and Recommendations section.

1.4 Cyber Security Features

1.4.1 Factory RBAC

The IED by default includes an RBAC which has two users. One is an Engineer and the other is a Security Administrator.

Important	**If the RBAC is not updated, the Engineer (default user) will auto-login with full engineer privileges to access all functions of the IED.** **If prompted to enter a password at the HMI, press the Cancel (C) button. This will allow you to have full engineer privileges.**

To activate the RBAC, download a new RBAC using SAT. This will allow you to add new users, and to remove or change the default user to control the auto-login.

Important	If you use the Factory RBAC, the default user will have full privileges and auto-login.

1.4.2 About Cyber Security

The philosophy of Cyber Security is to create a system view of security, and to track who has performed each action by identifying the person by their name and role.

Details of named users are stored in a secure centralized database, which is known as the Security Server. The Security Server contains details of the users, together with details of the Roles and the actions they performed. The database also records their passwords and/or their Key IDs. The IED also stores details of usernames, passwords, rights and roles – these being refreshed periodically from the Security Server.

Accordingly, instead of the user being granted access rights by virtue of knowing the password, they are now granted access rights as defined in the Security Server. These rights may be the same as other people who perform the same role; or they may be different, depending on the role assigned to the particular individual.

The individual item of substation equipment does not originate the details of every person who might have access rights. These details originate on the Security Server which manages the process of how those details are sent to the various devices. It does this so that the person who is attempting to access the device can be validated locally; and then be allowed to perform only those tasks which their pre-defined access rights allow. Using the Security Server means that new people can quickly have their details added to many devices quickly; and people who no longer have access can have their permissions removed from many devices just as quickly.

The Security Server works alongside a Gateway Server, which allow and/or prevent access to devices across a whole system architecture. These software tools also include various logging facilities; and allows auditors to view events, logs, reports and system alerts.

These new software-based tools and features make it much easier for managers to assign rights to roles and users, and to manage the system as a whole, rather than as many unrelated devices. In other words, system-level security.

- Configurable RBAC
- Device Hardening (disabling Unused Ports)
- Encrypted Password Use
- Simple UI Password
- Default User
- User Banner (message to the user to make sure he is configuring the intended device)
- Non-erasable logs and events
- Security Logs
- SNMP Alarms
- Risk Assessment Tool
- Ethernet Rate Limit Protection

1.5 Device and System Level Security

1.5.1 System Level Security

Figure 3 shows a very simplified view of system level security. In this situation, access is gained to the IED either by remote connection using a network or by direct connection to the IED or by using the buttons on the front panel of the IED. The IED is connected to a network, so includes the possibility of being connected to the internet or other open systems. Security is managed by the Security Server, which refreshes the list of approved usernames, passwords, roles and rights to the IEDs. The IED receives the username and password from the PC; and authenticates it against its database of permitted users. If access to the IED is allowed, it allows that user to access the IED, and perform the functions associated with their role and rights (these being refreshed periodically from the security server).

The Cyber Security architecture includes these components:

- Log Server (which records actions and messages, so they can be audited)
- Security Gateway (which control access to and from devices on the network)

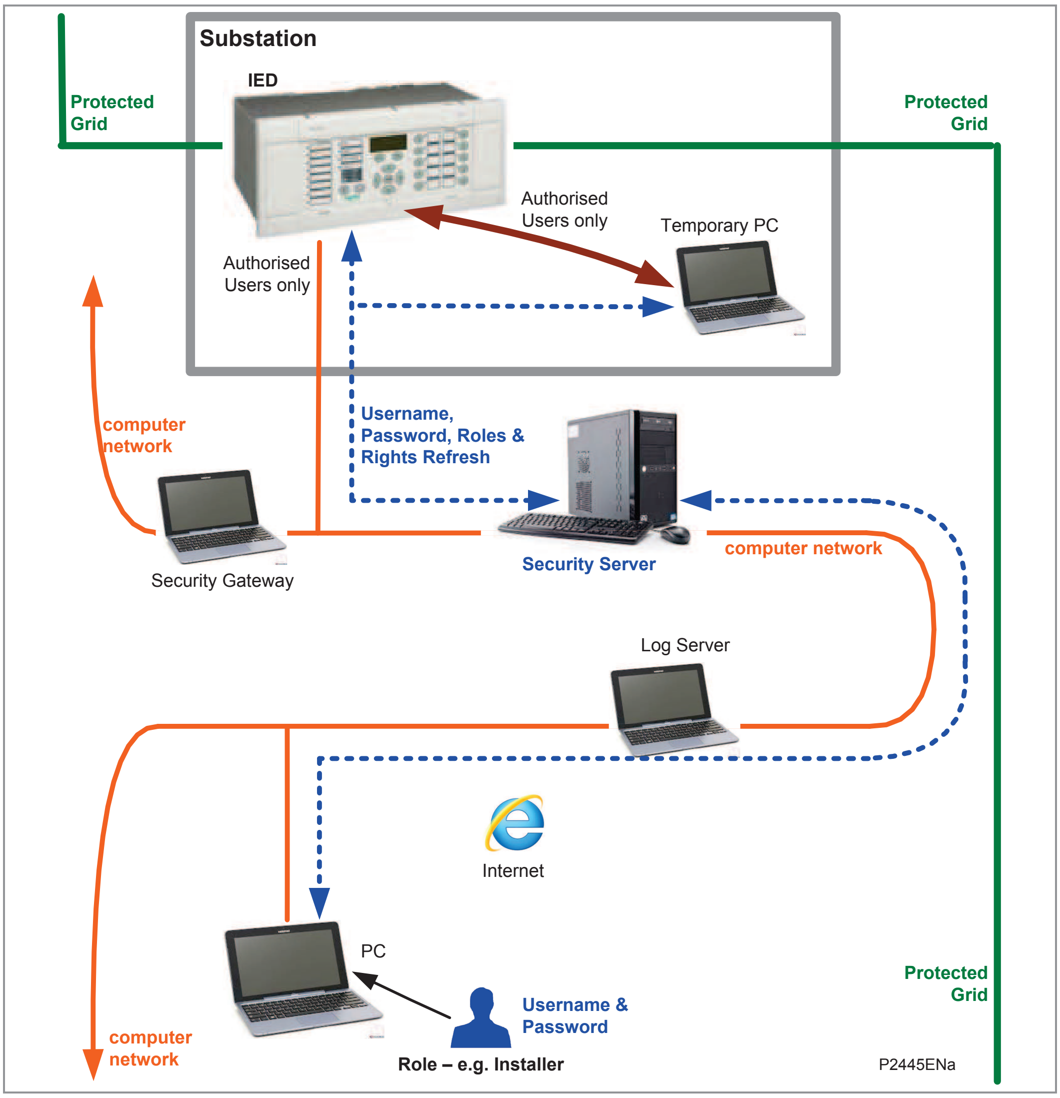

Figure 3 - System-level security (as per Cyber Security Phase II)

The Security Server manages a master copy of the database which determines access to the IED in the substation shown in Figure 3, plus any others IEDs which may be attached to the protected grid.

1.6 Encryption of Credentials

Usernames and passwords are secure as they are sent across networks in an encrypted form.

1.7 User Roles, Access Rights and Management

1.7.1 User Roles

Cyber Security is managed by network-based software that uses the concept of Roles and Rights. This is based on assigning authorized named users into one of a number of pre-defined roles (similar to job functions). This provides a useful way of managing users, roles and rights, with strong security features.

Different named roles are associated with different access rights. Roles and Rights are setup in a pre-defined arrangement, according to the IEC62351 standard, but customized to the MiCOM Px4x equipment.

When the user attempts to access an IED, they need to logon using their own username and their own password. The username/password combination is then checked against the records stored on the IED. If they are allowed to logon, a message appears which shows them what Role they have been assigned to. It is the role that defines their access to the relevant parts of the system.

There are a range of different roles, which provide a mix of access rights.

- The least access rights are in the “Viewer” role – this allows such a person to look at the data in an IED, but they can not make any changes it.
- The “Security Admin” role has additional access rights – this allows such a person to look at the data in an IED, as well as change it, manage files, configure the IED, define security settings and other functions.

A quick summary of these default roles is given here:

Role	Description
VIEWER	Can View what objects are present within a Logical-Device by presenting the type ID of those objects.
OPERATOR	An Operator can view what objects and values are present within a Logical-Device by presenting the type ID of those objects as well as perform control actions.
ENGINEER	An Engineer can view what objects and values are present within a Logical-Device by presenting the type ID of those objects. Moreover, an engineer has full access to Datasets and Files and can configure the server locally or remotely.
INSTALLER	An Installer can view what objects and values are present within a Logical-Device by presenting the type ID of those objects. Moreover, an installer can write files and can configure the server locally or remotely.
SECADM	Security Administrator can change subject-to-role assignments (outside the device) and role-to-right assignment (inside the device) and validity periods; change security setting such as certificates for subject authentication and access token verification.
SECAUD	Security Auditor can view audit logs
RBACMNT	RBAC Management can change role-to-right assignment.

Table 1 - Default user roles summary

A list of default Roles and a summary of their access Rights (as defined under IEC 62351-8) is shown in Table 2.

	Rights (IEC 62351-8 defaults)										
Roles	**VIEW**	**READ**	**DATASET**	**REPORTING**	**FILEREAD**	**FILEWRITE**	**FILEMNGT**	**CONTROL**	**CONFIG**	**SETTINGGROUP**	**SECURITY**
VIEWER	**X**			**X**							
OPERATOR	**X**	**X**		**X**				**X**			
ENGINEER	**X**	**X**	**X**	**X**		**X**	**X**		**X**		
INSTALLER	**X**	**X**		**X**		**X**			**X**		
SECADM	**X**	**X**	**X**			**X**	**X**	**X**	**X**	**X**	**X**
SECAUD	**X**	**X**		**X**	**X**						
RBACMNT	**X**	**X**					**X**		**X**	**X**	

Table 2 - Pre-defined roles (and rights) for IEC 62351-8 compliance

Note *Further details are provided in the Roles and Rights for IEC62351-8 and MiCOM Px4 section, which includes a detailed comparison of IEC and MiCOM Px4x Roles and Rights (see Table 7).*

Each authorized user needs to be placed into whichever ONE of these roles most suits their job description. It is possible to assign a user into a different role; and/or to change the rights associated with a particular role. This means that the administrator can change the access rights for one role; and this will affect ALL the users who are assigned to that role. Potentially this means that access rights for many people can be changed by the administrator making one change.

The combination of username, password and roles, means that a more detailed set of logs can be maintained, allowing an administrator to see which named people logged on and what they did whilst they were logged on.

1.7.2 Rights

In a similar way in which a set of pre-defined Roles have been created, a pre-defined set of Rights have been created.

These Rights give different permissions to look at what devices may be present, what those devices may contain, manage data within those devices (directly or by using files) and configure rights for other people.

A list of the pre-defined Rights is given here:

Right	Description
VIEW	Allows the subject/role to discover what objects are present within a Logical-Device by presenting the type ID of those objects. If this right is not granted to a subject/role, the Logical-Device for which the View right has not been granted shall not appear
READ	Allows the subject/role to obtain all or some of the values in addition to the type and ID of objects that are present within a Logical-Device;
DATASET	Allows the subject/role to have full management rights for both permanent and non-permanent Datasets;
REPORTING	Allows a subject/role to use buffered reporting as well as un-buffered reporting;

Right	Description
FILEREAD	Allows the subject/role to have read rights for file objects;
FILEWRITE	Allows the subject/role to have write rights for file objects. This right includes the FILEREAD right
CONTROL	Allows a subject to perform control operations;
CONFIG	Allows a subject to locally or remotely configure certain aspects of the server;
SETTINGGROUP	Allows a subject to remotely configure Settings Groups;
FILEMNGT	Allows the role to transfer files to the Logical-Device, as well as delete existing files on the Logical-Device;
SECURITY	Allows a subject/role to perform security functions at both a Server/Service Access Point and Logical-Device basis. To add Information about the concept of Rights.

Table 3 - Pre-defined rights

The relationship between Roles and Rights is shown in Table 2.

1.7.3 Management of Users and their Rights

It is possible to setup new Users and to assign them into Roles. This is done at a central location; which is normally not in the same location as any IEDs. Details of the usernames, passwords, roles and rights are refreshed to the relevant IEDs periodically.

For more information, please see the Security Server, Configuration and Security Administration Tool section.

1.8 Security Server, Configuration and Security Administration Tool

1.8.1 Concept

As well as changing how you manage access to IEDs, Cyber Security also deals with configuring tools, logging user access and managing all the security issues. It does this by using these functions:

- Security Server
- Security Gateway
- Logs Server
- Security Administration Tool (SAT) Software

1.8.1.1 Security Server

So far as MiCOM protection devices are concerned, the main functions of the Security Server are to manage authentication (through certificates, and adapted protocol to exchanges authentication information with other equipments).

To handle security data stored within the security server, a different PC uses the Security Administration Tool (SAT) software. The computer which runs the SAT will be connected to the IED or other protection device.

The SAT software operates in a centralized manner, covering different types of IED from Schneider Electric.

In addition, the Security Server needs to be compatible with other security servers as it may need to replicate, backup, send, receive or cache data from them. It also needs to translate protocols that may already be in place with other servers or protection equipment.

Whilst the Security Server generally uses Roles and Rights to determine permissions to access devices; it can also be used to give specific permissions to specific users on specific devices.

The Security Server can also manage a calendar (scheduler) to be able to change roles depending on the day and time.

As a centralized function, the Security Server will also be aware of devices connected to a grid (in terms of their manufacturer, model numbers, location, IP address, platform versions, etc). It can also show details of the connections between devices on the grid.

For more details of this, please refer to the SAT documentation.

1.8.1.2 Security Gateway

The Security Gateway controls how data is transferred between critical sections of the system. It performs a variety of tasks including making sure that:

- Relevant data (such as usernames and passwords) is transmitted in an encrypted form
- Connections to internet-based systems use a secure connection (e.g. https rather than just http)
- The gateway can manage load balancing and support high availability functions
- Firewall and anti-virus functions are fully supported
- Unused ports can be disabled (equipment hardening)

For more details of this, please refer to the Security Administration Tool (SAT) documentation.

1.8.1.3 Logs Server

The Security Logs server needs to store logs from each item of equipment. These logs are generated by the system, and can not be edited by the user. A variety of different items are recorded, these including: bad/faulty access attempts, login attempts, authentication errors, changes to roles, roles, users and access control lists, network backup and configuration changes, communication failures and so on. Further details of the items which are recorded are given in the Security Administration Tool (SAT) documentation. Samples of the possible events is shown in the Events section.

Alarms can be raised automatically in certain circumstances. Examples of these may include an excessive number of failed login attempts or a storage buffer becoming close to being full.

The Security Logs server stores log data for at least the time between two security audits (which can be at least 90 days). These log files are signed and can be sent to an external storage device. They can also be downloaded by a suitably authorized user.

Centralized log files are stored by the Security Logs server in an encrypted form. The date and time record of the log is determined by a centralized time reference.

For more details of this, please refer to the SAT documentation.

1.8.1.4 Security Administration Tool (SAT) Software

This Cyber Security documentation generally describes the security functions as they apply to MiCOM Px4x products. This documentation gives simple summary instructions as to how to access and use the Security Administration Tool (SAT) software. These instructions are intended to be a reminder as to how to use the SAT; and do not provide full details of the SAT software.

The SAT provides a variety of functions associated with using the software to manage a range of protection devices and deal with the security requirements associated with those tasks. As well as including managing users, roles and access permissions; this also includes the ability to record connected equipment and view the data logs associated with access to/from that equipment.

The details of how to use the SAT are provided in the SAT documentation:

SAT (Security Administration Tool) Documentation - User Guide

This will be available from the Schneider Electric website:

www.schneider-electric.com

The User Guide gives the functional and technical descriptions of user interfaces and a comprehensive set of instructions for installation and use of the SAT application. It has been designed to provide information for Site Engineers (who are responsible for the installation and maintenance of the SAT application), as well as Protection and Control engineers (who are concerned about how to select and apply the SAT to configure MiCOM devices).

SAT Requirements

The installation package installs the SAT, together with the Microsoft SQL Server 2008 R2 Express SP2 software.

The SAT installation software needs to be run by some-one with administrator privileges on a Windows XP, Windows 7 or Windows 8 operating system.

Data on the PC should be backed up before an installation is attempted, as data previously stored by a SAT application will be erased.

Permission to install the SAT is determined by the presence of a License Key (provided by Schneider Electric) linked to a Machine Information code; so the software will run on one approved PC.

For more details, please refer to the SAT User Guide.

SAT Functions Overview

The SAT allows an authorised user to Manage User Accounts, Roles, Permissions, Elements to Secure (ETS) and Security Server parameters, without connections to devices. This information is stored in the Microsoft SQL database, using an “offline” mode.

Offline mode is generally used for Administration tasks, such as Server Configuration, and the Management of User Accounts, and User Accounts/Roles Association, Roles and Elements to Secure Management.

Online mode is generally used for Communication tasks such as refreshing IED Lists, Displaying IED and SAM Logs and pushing RBAC and Security Policies.

Starting the SAT

An authorised user will usually start the SAT, by clicking the SAT icon on their desktop and logging in using their username and password.

SAT Interface Overview

The SAT Interface is split into two different workspaces.

A toolbar contains icons to allow commonly used functions to be run by clicking the mouse. It also includes details of the currently logged in username, as well as icons to resize the SAT window, and logout.

The SAT workspace contains a navigation banner and a view banner. The navigation banner allows a user to switch between different tabs which may be open. The view banner allows a user to view lists of User Accounts, Elements to Secure, Roles and Global Security and so on. Lists can be sorted using sort buttons which appear when necessary. Items on a list can be selectively shown/hidden by clicking the Filter Control icon.

SAT User Accounts

The SAT software provides one or more dialog boxes which contain the fields which are needed to define a User Account.

New accounts can be added (using the Add a User Account button).

An existing account can edited by double-clicking on it to open it.

An account can also be deactivated (by putting a X in the Deactivated check box); or completely suppressed by clicking the trash can icon in the same row of the table.

SAT Roles

The SAT software provides one or more dialog boxes which contain the fields which are needed to define a Role (such as ENGINEER). It also allows a security administrator to view Roles and User Accounts and create/edit/remove associations between Roles/Accounts and Accounts/Roles. This is done by highlighting the desired Role or Account and clicking the Associate button; then following the dialog boxes to associate one or more items together.

Note that User Accounts can also be associated with the pre-defined Global Security roles (Viewer, Operator, Engineer, Installer, SECADM, SECAUD and RBACMNT) defined in section 5.1 - Roles and their Access Rights.

SAT Communications Functions

The SAT can be used to communicate with devices on the network by using the Transfer Administration (TAT). This is accessed by clicking the TAT icon, and then the Open TAT View button, which then shows information from any devices located on the network in the Transfer Administration view.

A list of connected IEDs is shown in the Transfer Administration view. This can be updated by clicking the Refresh view. Logs from an individual IED can be viewed, by clicking on the IED in the list, then clicking the Visualize Logs option. SAM Logs can be viewed by highlighting the desired IED, then clicking the Visualize SAM Logs button. Logs can be exported by clicking on the Export Logs button.

Logs can be searched by entering a search criteria in the Search box and clicking the search icon.

RBAC and Security policies can also be send to one or more IEDs using the SAT. This operation is called Push Configuration; and is achieved by sending four xml files for Permissions, Roles, Users and Security Policies from the SQL database. To Push Configuration, highlight the IED you want to configure, then click the Push Configuration button from the Transfer Administration tab. You then need to create a Configuration Name, and the list of IEDs which have been updated (along with the version) will be shown in the updated SAM Logs list.

For more details, please refer to the SAT User Guide.

2 STANDARDS AND RECOMMENDATIONS

2.1 Schneider Electric Standards

Different versions of the Schneider Electric Cyber Security products meet various standards, depending on the relevant MiCOM product/software/hardware release.

The standards considered when we developed our Cyber Security products are:

- NERC Compliance
- IEEE 1686-2007
- IEC 62351
- BDEW White Paper Requirements
- NIST (National Institute of Standards and Technology)
- ISO/IEC 27000
- ISA 99
- CIGRE WG D2.22 Report

2.2 List of Standards and Recommendations

There are several standards and recommendations, which apply to substation cyber security (see Table 4).

	Country	
NERC CIP (North American Electric Reliability Corporation)	USA	Framework for the protection of the grid critical Cyber Assets
BDEW (German Association of Energy and Water Industries)	Germany	Requirements for Secure Control and Telecommunication Systems
ANSI ISA 99	USA	ICS oriented then Relevant for EPU completing existing standard and identifying new topics such as patch management
IEEE 1686	International	International Standard for substation IED cyber security capabilities
IEC 62351	International	Power system data and Comm. protocol
ISO/IEC 27002	International	Framework for the protection of the grid critical Cyber Assets
NIST SP800-53 (National Institute of Standards and Technology)	USA	Complete framework for SCADA SP800-82and ICS cyber security
CPNI Guidelines (Centre for the Protection of National Infrastructure)	UK	Clear and valuable good practices for Process Control and SCADA security

Table 4 - Recommendations and Standards applicable to cyber security

2.3 NERC Compliance

The North American Electric Reliability Corporation (NERC) created a set of standards for the protection of critical infrastructure. These are known as the CIP standards (Critical Infrastructure Protection). These were introduced to ensure the protection of Critical Cyber Assets, which control or have an influence on the reliability of North America’s bulk electric systems.

These standards have been compulsory in the USA for several years now. Compliance auditing started in June 2007, and utilities face extremely heavy fines for non-compliance.

The group of CIP standards is listed in Table 5.

CIP standard	Description
CIP-002-1 Critical Cyber Assets	Define and document the Critical Assets and the Critical Cyber Assets
CIP-003-1 Security Management Controls	Define and document the Security Management Controls required to protect the Critical Cyber Assets
CIP-004-1 Personnel and Training	Define and Document Personnel handling and training required protecting Critical Cyber Assets
CIP-005-1 Electronic Security	Define and document logical security perimeter where Critical Cyber Assets reside and measures to control access points and monitor electronic access
CIP-006-1 Physical Security	Define and document Physical Security Perimeters within which Critical Cyber Assets reside
CIP-007-1 Systems Security Management	Define and document system test procedures, account and password management, security patch management, system vulnerability, system logging, change control and configuration required for all Critical Cyber Assets
CIP-008-1 Incident Reporting and Response Planning	Define and document procedures necessary when Cyber Security Incidents relating to Critical Cyber Assets are identified
CIP-009-1 Recovery Plans	Define and document Recovery plans for Critical Cyber Assets

Table 5 - NERC CIP standards

The following sections provide further details about each of these standards, describing the associated responsibilities of the utility company and where the IED manufacturer can help the utilities with the necessary compliance to these standards.

2.3.1 CIP 002

CIP 002 concerns itself with the identification of:

- Critical assets, such as overhead lines and transformers
- Critical cyber assets, such as IEDs that use routable protocols to communicate outside or inside the Electronic Security Perimeter; or are accessible by dial-up.

Power utility responsibilities:	Schneider Electric's contribution:
Create the list of the assets	We can help the power utilities to create this asset register automatically. We can provide audits to list the Cyber assets

2.3.2 CIP 003

CIP 003 requires the implementation of a cyber security policy, with associated documentation, which demonstrates the management’s commitment and ability to secure its Critical Cyber Assets.

The standard also requires change control practices whereby all entity or vendor-related changes to hardware and software components are documented and maintained

Power utility responsibilities:	Schneider Electric's contribution:
To create a Cyber Security Policy	We can help the power utilities to have access control to its critical assets by providing centralized Access control. We can help the customer with its change control by providing a section in the documentation where it describes changes affecting the hardware and software.

2.3.3 CIP 004

CIP 004 requires that personnel having authorized cyber access or authorized physical access to Critical Cyber Assets, (including contractors and service vendors), have an appropriate level of training.

Power utility responsibilities:	Schneider Electric's contribution:
To provide appropriate training of its personnel	We can provide cyber security training

2.3.4 CIP 005

CIP 005 requires the establishment of an Electronic Security Perimeter (ESP), which provides:

- The disabling of ports and services that are not required
- Permanent monitoring and access to logs (24x7x365)
- Vulnerability Assessments (yearly at a minimum)
- Documentation of Network Changes

Power utility responsibilities:	Schneider Electric's contribution:
To monitor access to the ESP To perform the vulnerability assessments To document network changes	To disable all ports not used in the IED To monitor and record all access to the IEDthe access at all access points of the ESP

2.3.5 CIP 006

CIP 006 states that Physical Security controls, providing perimeter monitoring and logging along with robust access controls, must be implemented and documented. All cyber assets used for Physical Security are considered critical and should be treated as such:

Power utility responsibilities:	Schneider Electric's contribution:
Provide physical security controls and perimeter monitoring. Ensure that people who have access to critical cyber assets don’t have criminal records Schneider Electric's contribution.	Schneider Electric cannot provide additional help with this aspect.

2.3.6 CIP 007

CIP 007 covers the following points:

- Test procedures
- Ports and services
- Security patch management
- Antivirus

- Account management
- Monitoring
- An annual vulnerability assessment should be performed

Power utility responsibilities:	Schneider Electric's contribution:
To provide an incident response team and have appropriate processes in place	Test procedures; We can provide advice and help on testing. Ports and services; Our devices can disable unused ports and services Security patch management; We can provide assistance Antivirus; We can provide advise and assistance Account management; We can provide advice and assistance Monitoring; Our equipment monitors and logs access

2.3.7 CIP 008

CIP 008 requires that an incident response plan be developed, including the definition of an incident response team, their responsibilities and associated procedures.

Power utility responsibilities:	Schneider Electric's contribution:
To provide an incident response team and have appropriate processes in place.	Schneider Electric cannot provide additional help with this aspect.

2.3.8 CIP 009

CIP 009 states that a disaster recovery plan should be created and tested with annual drills.

Power utility responsibilities:	Schneider Electric's contribution:
To implement a recovery plan	To provide guidelines on recovery plans and backup/restore documentation

2.4 IEEE 1686-2007

IEEE 1686-2007 (often referred to only as IEEE 1686) is an IEEE Standard for substation IEDs cyber security capabilities. It proposes practical and achievable mechanisms to achieve secure operations.

The following features described in this standard apply to Schneider Electric Px40 relays:

- Passwords are 8 characters long and can contain upper-case, lower-case, numeric and special characters.
- Passwords are never displayed or transmitted to a user.
- IED functions and features are assigned to different password levels. The assignment is fixed.
- Record of an audit trail listing events in the order in which they occur, held in a circular buffer.
- Records contain all defined fields from the standard and record all defined function event types where the function is supported.
- No password defeat mechanism exists. Instead a secure recovery password scheme is implemented.
- Unused ports (physical and logical) may be disabled.

2.5 IEC 62351

This standard describes mainly, for our products:

- Secure communications for industrial protocols including IEC 61850, and how securing data access and transfer
- Data information to be logged, monitored and reported
- A model of role base access control

Parts 1 to 8 are published as Edition 1.0 and parts 9 and 10 are draft. The main parts of this standard are :

- Part-3: Communication Network and System Security – Profiles Including TCP/IP. These security standards cover those profiles used by ICCP, IEC 60870-5 Part 104, DNP 3.0 over TCP/IP, and IEC 61850 over TCP/IP
- Part -4: Communication Network and System Security – Profiles Including MMS. These security standards cover those profiles used by ICCP and IEC 61850.
- Part -5: Data and Communication Security – Security for IEC 60870-5 and Derivatives (i.e. DNP 3.0). These security standards cover both serial and networked profiles used by IEC 60870-5 and DNP.
- Part -6: Data and Communication Security – Security for IEC 61850 Profiles. This security Standards cover those profiles in IEC 61850-7-2 that are not based on TCP/IP – GOOSE, GSSE, and SMV.
- Part -7: Data and Communication Security – Management Information Base (MIB)Requirements for End-to-End Network Management. These security standards define Management Information Base (MIBs) that are specific for the power industry, to handle network and system management through SNMP-based capabilities.
- Part -8: Role-based access control for power system management. These security standards define a minimal set of Roles and Rights that are specific for the power industry to control access to data on the field, process and net-control-center level.

2.6 BDEW White Paper Requirements

This is known as the BDEW White Paper Requirements for Secure Control and Telecommunication Systems:2008

This document lists requirements, with references to controls of ISO/IEC 27002 about following categories :

- Patch management,
- Base system (system hardening, antivirus),
- Networks & communications ,
- Applications (user account management, authorizations, application protocols, web applications , logging, audit trails, alarms, self-test …),
- Development, Test and rollout
- Backup, recovery and disaster recovery

2.7 NIST (National Institute of Standards and Technology)

This is known as the NIST National Institute of Standards and Technology:

- NIST Special Publication 800-53: “Recommended Security Controls for Federal Information Systems and Organization”
- Special Publication 800-40 Version 2.0: "Creating a Patch and Vulnerability Management Program”
- Special Publication 800-82: "Guide to Industrial Control Systems (ICS) Security”

2.8 ISO/IEC 27000

This is known as the ISO/IEC 27000 series

- This covers Information security standards that provide best practice recommendations on information security management, risks and controls within the context of an overall Information Security Management System.

IS0 27002 describes code of good practices for Information Security Management. This standard is often used , with specific application to Industrial Security like in BDEW document.

2.9 ISA 99

This is known as the ISA 99

- This establish standards, recommended practices, reports and information that define procedures for implementing electronically secure manufacturing and control systems. It addresses all types of plants, facilities and systems in all industries such as DCS, PLC, SCADA, networked electronic sensing and monitoring systems …

2.10 CIGRE WG D2.22 Report

This is known as the CIGRE WG D2.22 Report (June 2009)

- Security Technologies Guideline. Practical guidance for deploying cyber security technology within electric utility data network .

3 MICOM P40 CYBER SECURITY IMPLEMENTATION

Schneider Electric P40 IEDs have always been and will continue to be equipped with state-of-the-art security measures. Due to the ever-evolving communication technology and new threats to security, this requirement is not static. Hardware and software security measures are continuously being developed and implemented to mitigate the associated threats and risks.

This section describes the current implementation of cyber security, valid for the release of platform software to which this manual pertains.

At the IED level, these cyber security measures have been implemented:

- Passwords
- Port Disablement
- Role Based Access Control (RBAC) Management
- Inactivity timer
- Storage of security events (logs) in the IED
- NERC-compliant default display

External to the IEDs, the following cyber security measures have been implemented:

- Antivirus and similar software
- Security patch management

3.1.1 Password Rules

- Passwords may be any length between 0 and 16 characters long
- Passwords may or may not be NERC compliant
- Passwords may contain any ASCII character in the range ASCII code 33 (21 Hex) to ASCII code 122 (7A Hex) inclusive
- Only one login is required for all the IED interfaces

3.2 Passwords

The use of a password is an important way in which secure access to a device can be maintained. Further details of password functions are given in these sections:

- Password Strengthening
- Password Management
- RBAC Recovery

3.2.1 Password Strengthening

Prior to the introduction of cyber security features, passwords could be very simple. These simple passwords were typically entered on the front panel of the MiCOM P40 IED. More complex passwords must be applied using a computer keyboard. This is because MiCOM P40 IEDs do not have a computer-style keyboard, so they can not be used to select complex alphanumeric characters.

Schneider Electric cyber security features mean that NERC compliant passwords can be used. This potentially results in a higher level of password complexity. These compliant passwords must include these requirements:

- At least one upper-case alpha character
- At least one lower-case alpha character
- At least one numeric character
- At least one special character (%,$...)
- At least six characters long

3.2.2 Password Management

The user is locked out temporarily, after a defined number of failed password entry attempts. The number of password entry attempts, and the blocking periods are configurable. These settings are shown in Table 6.

The first invalid password entry sets the attempts count (actual text here) to 1 and initiates an 'attempts timer'. Further invalid passwords during the timed period increments the attempts count. When the maximum number of attempts has been reached, access is blocked. If the attempts timer expires, or the correct password is entered *before* the 'attempt count' reaches the maximum number, then the 'attempts count' is reset to 0.

Once the password entry is blocked, a 'blocking timer' is initiated. Attempts to access the interface whilst the 'blocking timer' is running results in an error message, irrespective of whether the correct password is entered or not. Only after the 'blocking timer' has expired will access to the interface be unblocked, whereupon the attempts counter is reset to zero.

Attempts to write to the password entry whilst it is blocked results in the following message, which is displayed for 2 seconds.

```
NOT ACCEPTED
ENTRY IS BLOCKED
```

Appropriate responses achieve the same result if the password is written through a communications port.

The attempts count, attempts timer and blocking timer can be configured by the SAT (not by the IED), as shown in Table 6.

Setting	Cell col row	Units	Default Setting	Available Setting
Attempts Limit	25 02		3	0 to 3 step 1
Attempts Timer	25 03	Minutes	2	1 to 3 step 1
Blocking Timer	25 04	Minutes	5	1 to 30 step 1

Table 6 - Password blocking configuration

3.2.3 RBAC Recovery

RBAC recovery is the means by which the device can be reset to the factory-default RBAC settings if required. To obtain the recovery password the customer must contact the Schneider Electric Contact Center and supply the IED *Security Code*. The Contact Centre will use this to generate a Recovery Password which is then provided to the customer.

Caution **The “recovery” password gives you access to the Default RBAC Configuration. This action deletes all existing users (and their passwords), and restores the default username/password. The default user has an Engineer role.**

The security code is a 16-character ASCII string. It is a read-only parameter. The IED generates its own security code randomly. A new code is generated under the following conditions:

- On power up
- Whenever settings are set back to default
- On expiry of validity timer (see below)
- When the recovery password is entered

As soon as the security code is displayed on the LCD display, a validity timer is started. This validity timer is set to 72 hours and is not configurable. This provides enough time for the contact centre to manually generate and send a recovery password. The Service Level Agreement (SLA) for recovery password generation is one working day, so 72 hours is sufficient time, even allowing for closure of the contact centre over weekends and bank holidays.

To prevent accidental reading of the IED security code the cell will initially display a warning message:

```
PRESS ENTER TO
READ SEC. CODE
```

The security code will be displayed on confirmation, whereupon the validity timer will be started. Note that the security code can only be read from the front panel.

3.2.3.1 Entry of the Recovery Password (by setting your Default RBAC Configuration)

Caution	**The “recovery” password gives you access to the Default RBAC Configuration. This action deletes all existing users (and their passwords), and restores the default username/password. The default user has an Engineer role.**

The “recovery” password is intended for recovery only. It is not a replacement password that can be used continually. It can only be used once – for password recovery.

Entry of the recovery password causes the IED to reset the RBAC back to default. This is all it is designed to do.

On this action, the following message is displayed:

```
RBAC HAS
BEEN SET TO DEFAULT
```

The recovery password can be applied through any interface, local or remote. It will achieve the same result irrespective of which interface it is applied through.

3.3 Port Disablement (Equipment Hardening)

Potentially the availability of unused ports could provide a security risk. For this reason unused ports can be disabled (also known as equipment hardening). For more details, please see these sections:

- Disabling Physical Ports
- Disabling Logical Ports
- Ethernet Rate Limit Protection

3.3.1 Disabling Physical Ports

It is possible to disable unused physical ports. An Engineer role is needed to perform this action.

To prevent accidental disabling of a port, a warning message is displayed according to whichever port is required to be disabled. For example if rear port 1 is to be disabled, the following message appears:

```
REAR PORT 1 TO BE
DISABLED.CONFIRM
```

There are between two and four ports eligible for disablement:

- Front port
- Rear port 1
- Rear port 2 (not implemented on all models)
- Ethernet port (not implemented on all models)

Note *It is not possible to disable a port from which the disabling port command originates.*

3.3.2 Disabling Logical Ports

It is possible to disable unused logical ports. An Engineer role is needed to perform this action.

Note *The port disabling setting cells are not provided in the settings file*

Caution Disabling the Ethernet port will disable all Ethernet based communications.

If it is not desirable to disable the Ethernet port, it is possible to disable selected protocols on the Ethernet card and leave others functioning.

Three protocols can be disabled:

- IEC61850
- DNP3 Over Ethernet
- Courier Tunnelling

Note *If any of these protocols are enabled or disabled, the Ethernet card will reboot.*

3.3.3 Ethernet Rate Limit Protection

The Cyber Security software includes automatic Ethernet Rate Limit Protection against high levels of incoming Ethernet traffic for maintaining the performance of the system. There are various scenarios in which high levels of incoming Ethernet traffic may be experienced, including, for example cyber attacks based on denial of service methods.

The Cyber Security software also monitors both CPU and network usage. It then uses an algorithm to decide when activity has reached a “too busy” threshold so it can act appropriately. In order to mitigate against the risk of people successfully breaching any limits, the details of any such algorithms used are kept confidential.

3.4 Inactivity Timer

The MiCOM device runs an inactivity timer, which means that it records the last time an action was taken by a user who was logged in.

If the user does not perform an action within a pre-defined interval, the user will be logged off. This is to reduce the risk that a device can accidentally be left open to access by authorized people.

The inactivity timer is configurable by using the SAT.

3.5 Cyber Security Settings

Each MiCOM P40 IED includes a large number of possible settings – these determining how the device works. These settings are changed at the SAT.

4 HOW TO USE CYBER SECURITY FEATURES

The following sections shows the most common tasks associated with Cyber Security features.

For many of these tasks, the steps you take are the same as you have performed previously; with the main changes being in the steps you use to login and/or logout.

4.1 How to Logon

You can logon in two different ways:

At the Front Panel:

> Select your username and enter your front panel password at the prompt (this is a combination of the four arrow keys).

At the PC:

> Open the connection (such as within MiCOM S1 Studio), and you will be prompted for a logon. Select your username and enter your password.

4.2 How to Log Out

If you have been configuring the IED, you should 'log out'. You do this by going up to the top of the menu tree. When you are at the Column Heading level and you press the Up button, you may be prompted to log out with the following display:

```
DO YOU WANT TO
LOG OUT?
```

You will only be asked this question if your password level is higher than the fallback level.

If you confirm, the following message is displayed for 2 seconds:

```
LOGGED OUT
User Name
```

If you decide not to log out (i.e. you cancel), the following message is displayed for 2 seconds.

```
LOGOUT CANCELLED
User Name
```

4.3 How to Recover a Password

This is done by the Security Administrator at the SAT.

4.4 How to Disable a Port

It is possible to disable unused physical ports. An Engineer-role is needed to perform this action.

To prevent accidental disabling of a port, a warning message is displayed according to whichever port is required to be disabled. For example if rear port 1 is to be disabled, the following message appears:

```
REAR PORT 1 TO BE
DISABLED.CONFIRM
```

There are between two and four ports eligible for disablement:

- Front port
- Rear port 1
- Rear port 2 (not implemented on all models)
- Ethernet port (not implemented on all models)

Note *It is not possible to disable a port from which the disabling port command originates.*

Note *You can disable all the ports apart from the last available one. This is so that access to the device is not totally disabled.*

4.5 Disabling Logical Ports

It is possible to disable unused logical ports. A level 3 password is needed to perform this action.

Note *The port disabling setting cells are not provided in the settings file.*

Caution **Disabling the Ethernet port will disable all Ethernet based communications.**

If it is not desirable to disable the Ethernet port, it is possible to disable selected protocols on the Ethernet card and leave others functioning.

Three protocols can be disabled:

- IEC61850
- DNP3 Over Ethernet
- Courier Tunnelling

Note *If any of these protocols are enabled or disabled, the Ethernet card will reboot.*

4.6 RBAC Configuration

This includes tasks such as how to setup or change Roles, Rights, Users; and how to Change a Cyber Security Setting.

All these tasks are done at the SAT.

4.7 SNMP

SNMP allows security monitoring of events and alarms.

4.8 Security Logs

Enhanced Security Logs (and the level of detail) are configurable via the SAT, alwo allowing SysLog, TCP monitor.

4.9 User Interface (UI) Password

The User Interface (UI) Password is a simple combination of the four arrow keys on the front of the IED, up to a maximum of eight keys.

The user must login using the UI Password if they want to use the local HMI.

4.10 Default User

The privileges and the role of the Default User are set by the SAT.

The Default User will auto-login, when no username and password is provided, with the privileges set by the SAT.

Important	**If not changed by the SAT, the Default User is set as an Engineer.**

5 ROLES AND RIGHTS FOR IEC62351-8 AND MICOM PX4X

The following sections contain details of the Rights which are associated with each Role.

5.1 Roles and their Access Rights

A complete list of default Roles and their access Rights is shown in Table 7.

	Default Rights as defined by IEC 62351-8												Specific Rights for MiCOM Px4x						
Roles	VIEW	READ	DATASET	REPORTING	FILEREAD	FILEWRITE	FILEMNGT	CONTROL	CONFIG	SETTINGGROUP	SECURITY		Read Only (default_access_right)	IED Configuration (configuration_right)	HMI Display Settings (display_action_right)	Protection Configuration (protection_configuration_righ	IED Commands (control_right)	Reading of Records and Events (audit_read_right)	Extraction of Records and Events (audit_write_right)
VIEWER	X			X									X					X (i)	
OPERATOR	X	X		X				X					X		X		X	X (i)	X (i)
ENGINEER	X	X	X	X		X	X		X				X	X	X	X	X	X	X
INSTALLER	X	X		X		X			X				X	X	X	X	X	X	
SECADM	X	X	X			X	X	X	X	X	X		X						
SECAUD	X	X		X	X								X					X	X
RBACMNT	X	X					X		X	X			X						

Note X (i) indicate additional IEC 62351-8 compliance.

Table 7 - Pre-defined roles (and rights) for IEC 62351-8 and Px4x

Each of these Roles (viewer, operator, etc) are associated with certain Rights as shown in Table 7. There are default Rights which are defined by IEC 62351-8 and specific Rights which are associated with Schneider Electric MiCOM Px4x products

The MiCOM Px4x Rights have been categorized as default_access_right, configuration_right, display_action_right, protection_configuration_right, control_right, audit_read_right and audit_write_right.

Further details of the Px4x Rights are given in sections 5.2 to 5.8.

5.2 Read Only (default_access_right)

Read Only (default_access_right)	IED_DESC	IED_DATA	DISPLAY	IED_CONFIG	PROT_CONFIG	IED_COMMAND	AUDIT
Read	X	X	X	X	X	X	
Write	X						
Clear							

Read Only (default_access_right)	IED_DESC	IED_DATA	DISPLAY	IED_CONFIG	PROT_CONFIG	IED_COMMAND	AUDIT
Reset							
Select							
Send							
Accept							
Upload							
Download							

Note *IED_DESC is data which is used to identify the MiCOM P40 IED, such as the Serial Number and Model Number.*

5.3 IED Configuration (configuration_right)

IED Configuration (configuration_right)	IED_DESC	IED_DATA	DISPLAY	IED_CONFIG	PROT_CONFIG	IED_COMMAND	AUDIT
Read				X			
Write				X			
Clear							
Reset							
Select							
Send							
Accept							
Upload				X			
Download				X			

Note *IED_DESC is data which is used to identify the MiCOM P40 IED, such as the Serial Number and Model Number.*

5.4 HMI Display Settings (display_action_right)

HMI Display Settings (display_action_right)	IED_DESC	IED_DATA	DISPLAY	IED_CONFIG	PROT_CONFIG	IED_COMMAND	AUDIT
Read			X				
Write			X				

HMI Display Settings (display_action_right)	IED_DESC	IED_DATA	DISPLAY	IED_CONFIG	PROT_CONFIG	IED_COMMAND	AUDIT
Clear							
Reset							
Select			X				
Send							
Accept							
Upload							
Download							

Note *IED_DESC is data which is used to identify the MiCOM P40 IED, such as the Serial Number and Model Number.*

5.5 Protection Configuration (protection_configuration_right)

Protection Configuration (protection_configuration_right)	IED_DESC	IED_DATA	DISPLAY	IED_CONFIG	PROT_CONFIG	IED_COMMAND	AUDIT
Read					X		
Write					X		
Clear							
Reset							
Select							
Send							
Accept							
Upload							
Download							

Note *IED_DESC is data which is used to identify the MiCOM P40 IED, such as the Serial Number and Model Number.*

5.6 IED Commands (control_right)

IED Commands (control_right)	IED_DESC	IED_DATA	DISPLAY	IED_CONFIG	PROT_CONFIG	IED_COMMAND	AUDIT
Read						X	

IED Commands (control_right)	**IED_DESC**	**IED_DATA**	**DISPLAY**	**IED_CONFIG**	**PROT_CONFIG**	**IED_COMMAND**	**AUDIT**
Write						X	
Clear						X	
Reset						X	
Select						X	
Send							
Accept							
Upload							
Download							

Note *IED_DESC is data which is used to identify the MiCOM P40 IED, such as the Serial Number and Model Number.*

5.7 Reading of Records and Events (audit_read_right)

Reading of Records and Events (audit_read_right)	**IED_DESC**	**IED_DATA**	**DISPLAY**	**IED_CONFIG**	**PROT_CONFIG**	**IED_COMMAND**	**AUDIT**
Read							X
Write							
Clear							
Reset							
Select							X
Send							
Accept							
Upload							X
Download							

Note *IED_DESC is data which is used to identify the MiCOM P40 IED, such as the Serial Number and Model Number.*

5.8 Extraction of Records and Events (audit_write_right)

Extraction of Records and Events (audit_write_right)	**IED_DESC**	**IED_DATA**	**DISPLAY**	**IED_CONFIG**	**PROT_CONFIG**	**IED_COMMAND**	**AUDIT**
Read							
Write							
Clear							
Reset							
Select							
Send							X
Accept							X
Upload							
Download							

Note *IED_DESC is data which is used to identify the MiCOM P40 IED, such as the Serial Number and Model Number.*

6 EVENTS

The implementation of NERC-compliant cyber security necessitates the generation of a range of Event records, which log security issues such as the entry of a non-NERC-compliant password, or the selection of a non-NERC-compliant default display. Table 8 lists all Security events.

Event Value	Display
PASSWORD LEVEL UNLOCKED	USER LOGGED IN ON <int> LEVEL <n>
PASSWORD LEVEL RESET	USER LOGGED OUT ON <int> LEVEL <n>
PASSWORD SET BLANK	P/WORD SET BLANK BY <int> LEVEL <p>
PASSWORD SET NON-COMPLIANT	P/WORD NOT-NERC BY <int> LEVEL <p>
PASSWORD MODIFIED	PASSWORD CHANGED BY <int> LEVEL <p>
PASSWORD ENTRY BLOCKED	PASSWORD BLOCKED ON <int>
PASSWORD ENTRY UNBLOCKED	P/WORD UNBLOCKED ON <int>
INVALID PASSWORD ENTERED	INV P/W ENTERED ON <int>
PASSWORD EXPIRED	P/WORD EXPIRED ON <int>
PASSWORD ENTERED WHILE BLOCKED	P/W ENT WHEN BLK ON <int>
RECOVERY PASSWORD ENTERED	RCVY P/W ENTERED ON <int>
IED SECURITY CODE READ	IED SEC CODE RD ON <int>
IED SECURITY CODE TIMER EXPIRED	IED SEC CODE EXP -
PORT DISABLED	PORT DISABLED BY <int> PORT <prt>
PORT ENABLED	PORT ENABLED BY <int> PORT <prt>
DEF. DISPLAY NOT NERC COMPLIANT	DEF DSP NOT-NERC
PSL SETTINGS DOWNLOADED	PSL STNG D/LOAD BY <int> GROUP <grp>
DNP SETTINGS DOWNLOADED	DNP STNG D/LOAD BY <int>
TRACE DATA DOWNLOADED	TRACE DAT D/LOAD BY <int>
IEC61850 CONFIG DOWNLOADED	IED CONFG D/LOAD BY <int>
USER CURVES DOWNLOADED	USER CRV D/LOAD BY <int> GROUP <crv>
PSL CONFIG DOWNLOADED	PSL CONFG D/LOAD BY <int> GROUP <grp>
SETTINGS DOWNLOADED	SETTINGS D/LOAD BY <int> GROUP <grp>

Event Value	Display
PSL SETTINGS UPLOADED	PSL STNG UPLOAD BY <int> GROUP <grp>
DNP SETTINGS UPLOADED	DNP STNG UPLOAD BY <int>
TRACE DATA UPLOADED	TRACE DAT UPLOAD BY <int>
IEC61850 CONFIG UPLOADED	IED CONFG UPLOAD BY <int>
USER CURVES UPLOADED	USER CRV UPLOAD BY <int> GROUP <crv>
PSL CONFIG UPLOADED	PSL CONFG UPLOAD BY <int> GROUP <grp>
SETTINGS UPLOADED	SETTINGS UPLOAD BY <int> GROUP <grp>
EVENTS HAVE BEEN EXTRACTED	EVENTS EXTRACTED BY <int> <nov> EVNTS
ACTIVE GROUP CHANGED	ACTIVE GRP CHNGE BY <int> GROUP <grp>
CS SETTINGS CHANGED	C & S CHANGED BY <int>
DR SETTINGS CHANGED	DR CHANGED BY <int>
SETTING GROUP CHANGED	SETTINGS CHANGED BY <int> GROUP <grp>
POWER ON	POWER ON -
SOFTWARE_DOWNLOADED	S/W DOWNLOADED -

Where *int is the interface definition (UI, FP, RP1, RP2, TNL, TCP)*
prt is the port ID (FP, RP1, RP2, TNL, DNP3, IEC, ETHR)
grp is the group number (1, 2, 3, 4)
crv is the Curve group number (1, 2, 3, 4)
n is the new access level (0, 1, 2, 3)
p is the password level (1, 2, 3)
nov is the number of events (1 – nnn)

Table 8 - Security event values

Each event is identified with a unique number that is incremented for each new event so that it is possible to detect missing events as there will be a ‘gap’ in the sequence of unique identifiers. The unique identifier forms part of the event record that is read or uploaded from the IED.

Note *It is no longer possible to clear Event, Fault, Maintenance, and Disturbance Records*

7 GLOSSARY FOR CYBER SECURITY

Term	Meaning
AV	Anti virus
Business Service Layer	This layer coordinates the application, processes commands, make logical decision and calculation according to the business rules
C264	PACiS Calculator
CA	Certification Authority
CAT	Computer (C264) administration Tool , for replacing CMT
CET	Sepam Configurator
CIFS	Common Internet File System. Microsoft protocol use to share resources on a network.
CIP Standards	Critical Infrastructure Protection standards. NERC CIP standards have been given the force of law by the Federal Energy Regulatory Commission (FERC)
CMC	Certificates Management over CMS. An IETF RFC for distribution and registration of public keys and certificates
CMP	Certificates Management Protocol. An IETF RFC for distribution and registration of public keys and certificates (RFC 4210)
CRL	Certificates Revocation List. A list of revoked certificatesTheoretically still valid, but forbidden by the Security Administrator or the Security Server
Crypto Device	A small device embedding cryptographic capabilities and storage memory. It could be a smartcard, USB stick, serial dongle, etc, etc…
CSMS	Cyber Security Management System
Data Layer	Consists of the domain-related objects and their relationships that are manipulated by the user during the interaction with the software
DCS	Distributed Control System
ESP	Electronic Security Perimeter
ESS	Embedded Security Server
ETS	Element To Secure An ETS is an entity that represents a tool, utility or application function block that can be protected within the tool suite. It gathers a list of corresponding permissions with their set of values. This list is pre-defined and cannot be edited by any business user. A same ETS can be associated to many roles with different set of authorizations.
FTPS	FTP over TLS protocol. The classic file transfer protocol (FTP) secured using TLS tunneling.
FUSION	Project name for merge of previous ‘MIRROR’ and ‘New SEPAM’ projects
GAT	Gateway Administration Tool (not yet developed)
HIPS	Host intrusion Prevention System based on “white list” of accepted executables.
HMI	Human Machine Interface
IED	Intelligent Electronic Device. It is a power industry term to describe microprocessor-based controllers of power system equipments (e.g. Circuit breaker, transformer, etc)
IET	IED Engineering ToolSuite for FUSION project. Similar to SET but dedicated to IED.
IET	IED Engineering Tool.
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol

Term	Meaning
LOGS	All the operations related to the security (connection, configuration…) are automatically caught in events that are logged in order to provide a good visibility of the previous actions to the security administrators.
MAC	Mandatory Access Control.
NERC	North American Electric Reliability Council
NERO	NERC Electric Reliability Organization (ERO) certified by the Federal Energy Regulatory Commission to establish and enforce reliability standards for the bulk-power system.
NTP	The Network Time Protocol (NTP) is a protocol for synchronizing the clocks of computer systems.
OCSP	Online Certificate Status Protocol. An IETF RFC for online verification of certificates by servers (RFC 2560).
PAP	Policy Administration Point. Software entity that manage the security Policy
PDP	Policy Decision Point. Software entity that evaluates the applicable policy and takes an authorization decision
PEP	Policy Enforcement Point. Software entity that performs access control and enforces authorization decision.
PIP	Policy Information Point. Software entity acting as an information source for the PDP.
PKI	Public Key infrastructure
PSP	Physical Security Perimeter
PSTN	Public Switched Telephone Network (RTC in French)
RA	Registration Authority
RBAC	Role Based Access Control Authentication and authorization mechanism based on roles granted to a user. Roles are made of rights, themselves being actions that can be applied on objects. Each user's action is authorized or not based on his roles
Roles	A role is a logical representation of a person activity. This activity authorizes or forbids operations within the tool suite thanks to permissions that are associated to the role. A role needs to be attached to a user account to have a real purpose.
RTCS	Real Time Certificate Status. Facility. An IETF draft for online certificates validation.
SAM	Security Administration Module. Device in charge of security management on an IP-over-Ethernet network.
SAS	Substation Automation Solutions / System
SAT	Security Administration Tool TSF based application used to define and create security configuration
SAU	Security Administration Utility
SCEP	Simple Certificate Enrollment Protocol. An IETF draft for distribution and registration of public keys and certificates
Scopes	The nodes of the hierarchy are viewed as scopes and can be secured independently. Each node could include some roles and user accounts defined in the tool suite and create a specific security policy.
SCVP	Server-based Certificate Validation Protocol. An IETF RFC for online certificates validation.
Secured IED	Devices embedding security mechanisms defined in the security architecture document
Security Administrator	A user of the system granted to manage its security
SET	System Engineering Tools. New Tools in place of SCE and SMT, to deal with complete life cycle for Systems (design, realization, testing, commissioning, maintenance)
SFTP	A secured file transfer protocol based on SSH.

Term	Meaning
SMB	Server Message Block. Microsoft protocol for network resources sharing. Called CIFS on NT
SMT	Substation Management Tool (previously used on PACIS project)
SMTP	Simple Mail Transfer Protocol (SMTP) is an Internet standard for electronic mail (e-mail) transmission across Internet Protocol (IP) networks.
SNMP	Simple Network Management Protocol (SNMP) is an "Internet-standard protocol for managing devices on IP networks
SSH	Secured Shell. A secured encrypted network protocol for remote administration of computers
SSL	Secured Socket Layer
SSL	See TLS (TLS is based on SSLv3)
SSO	Single Sign On
SUI	Substation User Interface
TAT	Transfer Administration Tool
TBD	To be defined
TLS	Transport Layer Security network protocol successor to SSL
TLS	Transport Layer Security. Creates encrypted tunnel for TCP connections. Can guarantee authentication when used in a PKI.
TSF	Tool Suite Foundation. Common framework for SET and IET. Mainly 3 parts Core, Workbench (for standardized HMI), Utilities (applicative components like trace viewer, installer)
UA	User Account. A user account is a logical representation of a person with some configurable parameters. It includes information about the user identity and gives him a login to be recognized within the tool suite. A user account is principally interesting when it is associated to some roles that will grant him authorizations.
Unsecured IED	Relay/IEDs with no security mechanisms.
VDS	Virtual Device Solution
VPN	Virtual Private Network (a secure private connection established on a public network or other unsecured environment).
XACML	eXtensible Access Control Markup Language. An OASIS standard defining an XML access control policy implementation.
XKMS	XML Keys Management Specifications. A 3C standard, XML based, for distribution and registration of public keys and certificates