CYBER SECURITY

CHAPTER 18

Applicability	
Date:	01/2020

Products covered by this chapter:

This chapter covers the specific versions of the MiCOM products listed below.
This includes **only** the following combinations of Software Version and Hardware Suffix.

Hardware Suffix:	
P141/P142/P143	L or later
P145	M or later
P241	L or later
P242/P243	M or later
P341	L or later
P342	L or later
P343/P344/P345	M or later
P391	A or later
P445	L or later
P44x (P442/P444)	M or later
P44y (P443/P446)	M or later
P54x (P543/P544/P545/P546)	M or later
P642	L or later
P643/P645	M or later
P742	L or later
P741/P743	M or later
P746	M or later
P841A (one circuit breaker)	M or later
P841B (two circuit breakers)	M or later
P849	M or later

Software Version:	
P14x (P141/P142/P143/P145)	B5 or later
P24x (P241/P242/P243)	D2 or later
P341	B3/E3 or later
P34x (P342/P343/P344/P345/P391)	B3 or later
P44x (P442/P444)	E3 or later
P44y (P443/P446)	K1 or later
P445	K1 or later
P54x (P543/P544/P545/P546)	K1 or later
P64x (P642/P643/P645)	B4 or later
P74x (P741/P742/P743)	B1 or later
P746	B5/C5 or later
P841A (one circuit breaker)	L1 or later
P841B (two circuit breakers)	K1 or later
P849	B2 or later

Connection Diagrams:	This chapter may use any of these connection diagrams:
P14x (P141, P142, P143 & P145):	10P141xx (xx = 01 to 02) 10P142xx (xx = 01 to 05) 10P143xx (xx = 01 to 11) 10P145xx (xx = 01 to 11)
P445:	10P445xx (xx = 01 to 04)
P44x (P442 & P444):	10P44201 (SH 1 & 2) 10P44202 (SH 1) 10P44203 (SH 1 & 2) 10P44401 (SH 1) 10P44402 (SH 1) 10P44403 (SH 1 & 2) 10P44404 (SH 1) 10P44405 (SH 1) 10P44407 (SH 1 & 2)
P44y:	10P44303 (SH 01 and 03) 10P44304 (SH 01 and 03) 10P44305 (SH 01 and 03) 10P44306 (SH 01 and 03) 10P44600 10P44601 (SH 1 to 2) 10P44602 (SH 1 to 2) 10P44603 (SH 1 to 2)
P54x (P543, P544, P545 & P546):	10P54302 (SH 1 to 2) 10P54303 (SH 1 to 2) 10P54304 (SH 1 to 2) 10P54400 10P54404 (SH 1 to 2) 10P54405 (SH 1 to 2) 10P54502 (SH 1 to 2) 10P54503 (SH 1 to 2) 10P54504 (SH 1 to 2) 10P54600 10P54604 (SH 1 to 2) 10P54605 (SH 1 to 2) 10P54606 (SH 1 to 2)
P64x (P642, P643 & P645):	10P642xx (xx = 1 to 10) 10P643xx (xx = 1 to 6) 10P645xx (xx = 1 to 9)
P746:	10P746xx (xx = 00 to 21)
P841:	10P84100 10P84101 (SH 1 to 2) 10P84102 (SH 1 to 2) 10P84103 (SH 1 to 2) 10P84104 (SH 1 to 2) 10P84105 (SH 1 to 2)
P849:	10P849xx (xx = 01 to 06)

Notes:

CONTENTS

TABLES

FIGURES

1. OVERVIEW

1.1 Definition

Cyber security is a domain that addresses attacks on or by computer systems and through computer networks that can result in accidental or intentional disruptions.

Cyber security addresses not only deliberate attacks, such as from disgruntled employees, industrial espionage, and terrorists, but also inadvertent compromises of the information infrastructure due to user errors, equipment failures, and natural disasters.

1.2 Introduction to Cyber Security

The objective of cyber security is to provide increased levels of protection for information and physical assets from theft, corruption, misuse, or accidents while maintaining access for their intended users.

To achieve this objective the owner of the grid must take into account Cyber Security at every level of his organization by the management of an ongoing process that encompasses procedures, policies, technical (software, and hardware asset) and regulatory constraints.

The following diagram outlines some of the associated topics.

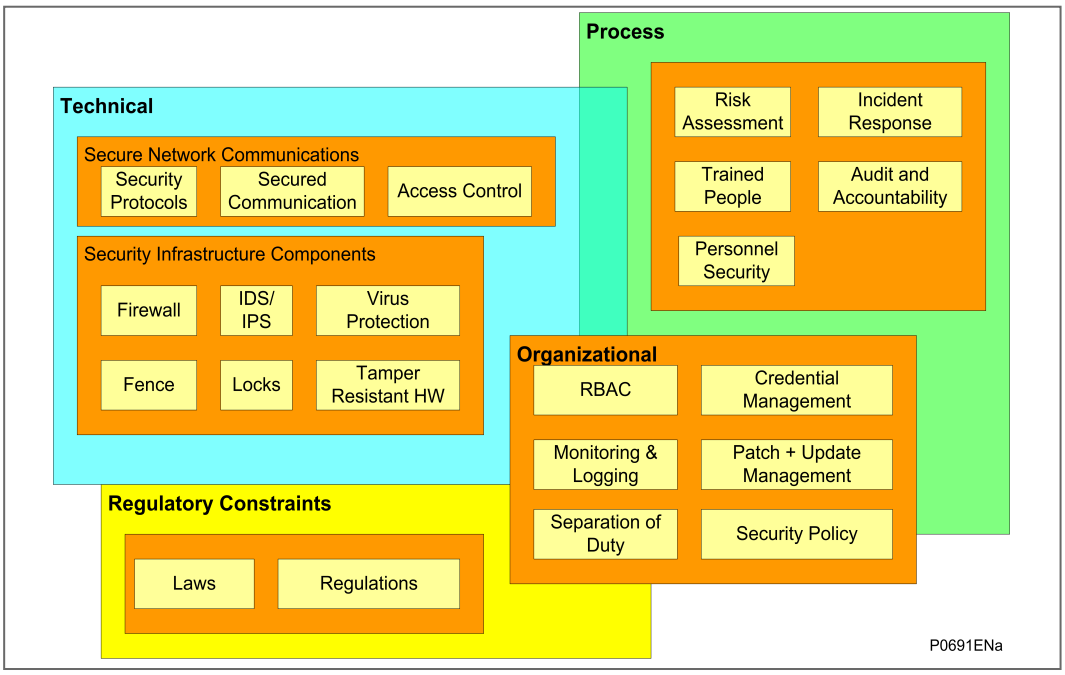

Figure 1 - Associated topics

The asset owner needs to run a continuous improvement process as outlined here:

Figure 2 - Continuous improvement process

No single solution can provide adequate protection against all cyber attacks on the control network. Schneider Electric recommends employing a “defense in depth” approach using multiple security techniques to help mitigate risk.

A secured system is to offer:

- Detective controls: Monitor and record specific types of events: Security logs, Intrusion, detection systems, Video Surveillance etc.
- Preventive controls: Help blocking or controlling specific event: Antivirus, White listing, Firewall etc.
- Recovery controls: Help achieve Business continuity and Disaster recovery planning objectives in case of an incident: Backup and Restore solution.

As protective relay vendor, Schneider Electric helps the grid owner to achieve by providing technical features inside the IED, described in the next chapters.

Important
This product contains a cyber-security function, which manages the encryption of the data exchanged through some of the communication channels. The aim is to protect the data (configuration and process data) from any corruption, malice, attack. Subsequently, this product might be subject to control from customs authorities. It might be necessary to request special authorization from these customs authorities before any export/import operation. For any technical question relating to the characteristics of this encryption please contact your Customer Care Centre - www.schneider-electric.com/ccc.

1.3 Roles, Rights and relationship between IEC62351 and MiCOM Px4x

1.3.1 Role Based Access Control (RBAC)

The Role Based Access Control (RBAC) is a method to restrict resource access to authorized users. RBAC is an alternative to traditional Mandatory Access Control (MAC) and Discretionary Access Control (DAC).

A key feature of RBAC model is that all access is through roles. A role is essentially a collection of permissions, and all users receive permissions only through the roles to which they are assigned, or through roles they inherit through the role hierarchy.

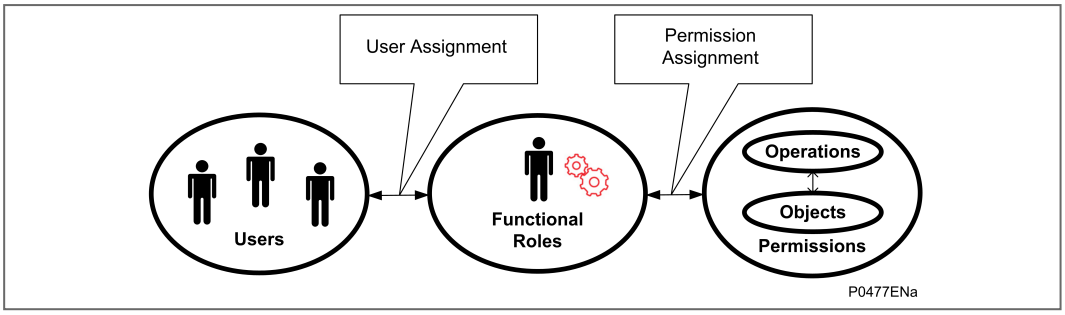

Figure 3 - RBAC role structure

Roles are created for various job activities. The **Permissions**, to perform certain operations, are assigned to specific roles. **Users** are assigned particular roles, and through those role assignments acquire the computer permissions to perform particular computer-system functions. Since users are not assigned permissions directly, but only acquire them through their role (or roles), management of individual user rights becomes a matter of simply assigning appropriate roles to the user's account; this simplifies common operations, such as adding a user, or changing user's account.

RBAC defines four different concepts:

RBAC Standard Definition	Description
Object	An **object** can represent information containers (e.g. files, directories in an operating system, tables and views in a database management system) or device resources, such as IEDs.
Subject	A **subject** is a user of the system. Note that a subject can be a person, or an automated agent / device.
Right	A **right** is the ability to access an object in order to perform certain operations (e.g. setting a data or reading a file)
Role	A **role** defines a certain authority level in the system. Rights are assigned to roles.

Table 1 - RBAC object, subject, rights and roles definitions

RBAC defines three primary rules:

RBAC Rule	Description
Role assignment	A subject can exercise a permission only if the subject has selected or been assigned a role.
Role authorization	A subject's active role must be authorized for the subject. With rule 1 above, this rule ensures that users can take on only roles for which they are authorized.
Permission authorization	A subject can exercise permission only if the permission is authorized for the subject's active role. With rules 1 and 2, this rule ensures that users can exercise only permissions for which they are authorized.

Table 2 - RBAC permission and authorization rules

1.3.2 User Roles

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 tries to access an IED, they need to login 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 login, 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.

The default user roles for MiCOM Px4x are shown 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.
SECADM	Security Administrator can change subject-to-role assignments (outside the device) and role-to-right assignment (inside the device) and security policy setting; change security setting such as certificates for subject authentication and access token verification.
SECAUD	Security Auditor can view audit logs

Table 3 - Default user roles summary for MiCOM Px4x

Each authorized user must be placed into at least ONE of these roles that 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.

It is possible for MiCOM Px4x to create the customized user roles.

1.3.3 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 for IEC 62351-8 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
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

Right	Description
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 4 - Pre-defined rights for IEC 62351-8

The specific Rights for MiCOM Px4x are listed below. These are dependent on the IED data type. Please refer to each product MD file (Menu Database) for the IED data type.

Rights	Authorized Actions to IED	IED_ DESC	IED_ DATA	DISPLAY	IED_ CONFIG	PROT_ CONFIG	IEC_ COMMAND	AUDIT	IED_ FN_ KEY	IED_ CLEAR
Read Only (SAT default_ access_right)	Read	x	x	x	x		x			
	Write	x								
IED Configuration (SAT configuration_ right)	Read / Write / Upload / Download				x					
HMI Display Settings (SAT display_ action_right)	Read / Write / Select			x						
Protection Configuration (SAT protection_ configuration_ right)	Read / Write					x				
IED Commands (SAT control_ right)	Read / Write / Clear / Reset / Select						x			
Reading of Records & Events (SAT audit_read_ right)	Read / Select / Upload							x		
Extraction of Records and Events (SAT audit_write_ right)	Send / Accept							x		
IED Function Key (SAT fn_key_ access_right)	Write								x	

Rights	Authorized Actions to IED	IED_ DESC	IED_ DATA	DISPLAY	IED_ CONFIG	PROT_ CONFIG	IEC_ COMMAND	AUDIT	IED_ FN_ KEY	IED_ CLEAR
IED Records Clear (SAT clear_right)	Read / Write / Clear									x

Table 5 - Specific rights for MiCOM Px4x

1.3.4 Roles and their Access Rights

A complete list of the Roles and their access Rights is shown in this table:

Rights		Roles				
		VIEWER	OPERATOR	ENGINEER	SECADM	SECAUD
Pre-defined Rights for IEC 62351	VIEW	x	x	x	x	x
	READ		x	x	x	x
	DATASET			x		
	REPORTING	x	x	x		x
	FILEREAD					x
	FILEWRITE			x	x	
	FILEMNGT			x	x	
	CONTROL		x		x	
	CONFIG			x	x	
	SETTINGGROUP				x	
	LOGS				x	x
	SECURITY				x	
Specific Rights for MiCOM Px4x	Read Only	x	x	x		x
	IED Configuration			x		
	HMI Display Settings		x	x		
	Protection Configuration			x		
	IED Commands		x	x		
	Reading of Records and Events	x	x	x		x
	Extraction of Records and Events		x	x		x
	IED Function Key		x	x		
	IED Clear			x		

Table 6 - Pre-defined roles (and rights) for IEC 62351-8 and MiCOM Px4x

Important
The reason why these are described as Default, is that it is possible to change the definitions of Roles and Rights, using the full version of the SAT software. Depending on the work done by the system administrator, it is possible that your own situation may vary from these initial recommendations.

1.4 Security Administration Tool (SAT) Software

Important
This can only be used with Px4x relays with cyber security CSL1 features.

Important
For Dual Ethernet cards the SAT functionality is available from communication interface 1. The connection to the SAT would be available from interface 2 only when interface 1 is disconnected from the network.

The Security Administration Tool (SAT) is the security configuration tool of MiCOM Px4x equipment. It allows the security administrator to define the security policy to the IEDs.

The Security Administrator manages RBAC and security policies data. Security Administrator defines needs to protect devices in accordance with user privileges. Thus, the system security can be configured easily and precisely.

The SAT is used by the Security Administrator to manage the system's security database and deploys security configurations to IED(s).

The SAT allows to Manage User Accounts, Roles, Permission, Elements to Secure (ETS) and Security Server parameters without connection with devices. Information is store on the MS SQL database. This is the Offline mode. SAT allows devices management connected on network. This is the online mode.

The Role Based Access Control (RBAC) is a method to restrict resource access to authorized users. Please refer to the "System RBAC Management" section for more details.

The following table contains the main user functions of the SAT:

Category	User Function	Note
Offline General Administration	User Accounts Management	User Account Functions: * Creation * Edition * Suppress * Viewing * Sorting * Filtering
	Server Configuration	
	Users Accounts & Roles association Management	Associate a role to the user account
Offline Advanced Administration	Roles Management	Roles Functions: * Creation * Edition * Suppress * Viewing * Sorting
	Element To Secure (ETS) Management	Define ETS which are in fact the PACiS assets present in the project (C264, PACiS Gateway, ECOSUI, IED and SAM). Add, Suppress and Sort permissions associated with the ETS.
	Global Security Management	The Global Security allows scope(s) and associate or disassociate role(s) management for each user account. The security administrator manages the current scope by the Roles: * View Roles List, User Account List and associations User-Roles or Role-Users * Associate / dissociate role(s) for each User

Category	User Function	Note
		Account * Add / Suppress User account(s) for each Role
	Permission access	Define parameters: * Password validity * Inactivity period * Automatic logout period * Maximum attempts of login and lockout period
Communication	Refresh IED list	
	Display IED Logs	
	Display SAM Logs	
	Push RBAC and Security Policies	Send Security Configuration to all Devices integrating Security features.

Table 7 - Main SAT user functions

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

SAT (Security Administration Tool) Documentation - User Guide

This is available from the Schneider Electric website: www.schneider-electric.com.

2. MICOM PX4X CYBER SECURITY IMPLEMENTATION

Considered some users may not want to use the cyber security, Schneider Electric offers MiCOM Px4x relays with CSL0 and CSL1 as below:

CSL0: Simple password management, No SAT required.

CSL1: Advanced cyber security, SAT required.

This depends on the model number, as CSL1 is depend on the Ethernet communication. Hence if the IED if supports only legacy protocol this will be CLS0 default as. The digit position number 9 (protocol options) in the Cortec / model number is used to distinguish it.

Protocol Option Number	Protocol Options	Cyber Security Options
1	K-Bus/Courier	CSL0
2	Modbus	CSL0
3	IEC 60870 -5 - 103	CSL0
4	DNP3.0	CSL0
6	IEC 61850 Edition 1 / 2 and Courier via rear K-Bus/RS485	CSL0
7	IEC 61850 Edition 1 / 2 and CS103 via rear port RS485	CSL0
B	IEC 61850 Edition 1 / 2 and DNP3oE and DNP Serial	CSL0
G	IEC 61850 Edition 1 / 2 and Courier via rear K-Bus/RS485	CSL1
H	IEC 61850 Edition 1 / 2 and CS103 via rear port RS485	CSL1
L	IEC 61850 Edition 1 / 2 and DNP3oE and DNP3 serial	CSL1

Table 8 - MiCOM Px4x protocol options for cyber security options

Important
Except for Courier tunneling via secured communication (TLS), the device does not have the capability to transmit data encrypted using the following protocols:
IEC 61850, DNP3 over Ethernet, Courier serial, Modbus serial, IEC60870-5-103 serial, and DNP3 serial.
If other users gained access to your network, transmitted information can be disclosed or subject to tampering.
For transmitting data over an internal network, physically or logically segment the network and restrict access using standard controls such as firewalls and other relevant features supported by your device such as IPTable whitelisting.
For transmitting data over an external network, encrypt protocol transmissions over all external connections using an encrypted tunnel, TLS wrapper or a similar solution.

2.1 MiCOM Px4x with CSL1 - Advanced Cyber Security

For MiCOM Px4x IEDs which support CSL1, this means the IED supports advanced user account right management. Moreover, the IED supports security logs/events and secure administration capability.

If you want to use cyber security, you need to order the IED that supports CSL1. In this case, the Security Administration Tool (SAT) is required for RBAC configuration.

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

- Passwords management (via the SAT)
- RBAC Management (via the SAT)
- User Locking
- Inactivity Timer
- RBAC recovery
- Port Disablement (via Easergy Studio or the front panel)
- Security Logs

2.1.1 Password Management (via the SAT)

For the IED if CSL1 supported, there are two types of password possible for the IED access: alphanumeric password or Arrow Key password.

The alphanumeric password is only settable via the SAT:

- Passwords may be any length between 1 and 32 characters long
- Passwords may contain any ASCII character in the range ASCII code 33 (21 Hex) to ASCII code 122 (7A Hex) inclusive
- Passwords may or may not be NERC/IEEE 1686 compliant
- The alphanumeric password will used for courier client access

For more details about NERC/IEEE 1686 password compliant, please check the standard.

The Arrow Key password is only settable via the SAT:

- The Arrow Key password is a combination of the four arrow keys on the front panel
- The Arrow Key password may be any length between 1 and 8 arrow keys long
- The Arrow Key password can only be used in the front panel
- The user also can disable the Arrow Key password by not setting it

Important
If the Arrow Key password is not configured, the alphanumeric password will be used for the front panel access. In this case, alphanumeric passwords longer than 16 characters are not allowed.
Easergy Studio and the front panel are not allowed to change the password.

Important
The Schneider Electric password policy is one of the key elements of the Cyber Security Policy.
Good practice to improve the Password definition:
- Use common Cyber Security Good Practice for password complexity definition by using strong passwords.
- Change All Passwords from their default value when taking the protection device into use. (User must change password after first login).
- Change Passwords regularly. (User must update password after a certain period of time).
- Use NERC Compliant password as much as possible.
- Enforce the use of strong and complexes Password as : Caps characters + Lowercases characters + Numbers + Special characters in one password.
- Set the minimum password length to 10 characters.
- Switch off all Comm port not use on the device, if possible.
- Do not reuse old passwords.
- All P40 relays installed before January 2020 should be checked separately case by case to confirm the Cyber Security conformity to Standard/country law.
All user must be aware of best practice concerning passwords, these include:
- Not Sharing personal passwords.
- Not displaying passwords during password entry.
- Not transmitting passwords in email or by other means.
- Not saving the passwords on PC's or other devices.
- Not written password on any supports.
- Regularly reminding users about best practices concerning password.

2.1.2 RBAC Management (via the SAT)

By default, the IED includes a factory RBAC which has three users, and for each user, the Rights depend on the user Role. Please refer to the ***Roles and their Access Right***s section for more details.

Username	Role	Default password
SecurityAdmin	SECADM	AAAAAAAA
EngineerLevel	ENGINEER	AAAA
OperatorLevel	OPERATOR	AAAA

Table 9 - Factory RBAC

A Local Default Access function also available for the default RBAC, with the VIEWER role, which allows everyone login the IED in the front panel with VIEWER role. For more details about the Local Default Access function, please refer to the ***Local Default Acces***s section.

For more information about how the SAT management the RBAC and cyber security policies, please see the 1.4 - Security Administration Tool (SAT) Software section.

2.1.3 User Locking

The user is locked out temporarily, after a defined number of failed password entry attempts.

Important
If a user is locked out, the block is applied to that named user and to the all IED interfaces. The blocking of one user, does not apply blocks to others.
If the user entry is blocked, recover the RBAC or push a new RBAC will not reset the blocked user entry, but IED reboot will reset the blocking time and attempts count, so the user entry will be unblocked.

An invalid password entry will display a 'Login Failed PW Incorrect' message for 2s. It also reduces the Attempts Remaining Counter (Attempts Remain) by 1 and it remains at this level

until the interface inactivity timer expires (CSL0 models) or until the Password Attempts Timer configured in SAT expires (CSL1 models) or another password entry is made. If Attempts Remain equals 1 then a '1 Attempt Left' warning will also be issued for 2s. When Attempts Remain equals 0 then a 'USER LOCKED OUT' warning is displayed for 2s and access for that user is blocked. If the Blocking Timer expires, or the correct password is entered before Attempts Remain reaches zero, then the Attempts Remain is reset to the Attempts Limit.

Once the user entry is blocked, the Blocking Timer is initiated. If the locked out user is selected whilst the Attempts Remain is zero a 'USER LOCKED OUT' error message is displayed.

2.1.4 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 unauthorized people.

The inactivity timer is separate for each interface.

The inactivity timer is configurable by using the SAT.

Important
In case of a connection through an Ethernet interface, the actual inactive time depends on the setting value of both "Minimum inactivity period" & "[0E A7] ETH Tunl Timeout", the smaller value of both timers will be applied.

Refer to the 2.1.8 - Common Cyber Security Settings section for more details.

2.1.5 RBAC Recovery

RBAC recovery is the means by which the device can be reset to the factory RBAC settings if required. To obtain the recovery password, the customer must go to www.schneider-electric.com/ccc to raise a recovery password request and supply the IED Security Code.

Caution
The “recovery” password gives you access to the Factory RBAC Configuration. This action deletes all existing users (and their passwords), and restores to Factory RBAC Configuration. Recover the RBAC does not affect relay proper settings and does not provoke reboot of the relay - the protection functions of the relay are always maintained.

2.1.5.1 Generate Security Code

The security code is a 16-character ASCII string. It is a read-only parameter. The IED generates its own random security code. This is when a new code is generated:

- On power up
- On expiry of validity timer (see below)
- When the recovery password is entered

As soon as the security code is first displayed on the LCD display, a validity timer is started. This validity timer is set to 120 hours and is not configurable. The validity timer is not reset if you request a subsequent code within the 120 hour period.

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

```
PRESS ENTER TO
READ SEC. COD
```

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.

Important
The recover password will be invalid once the new Security Code is generated, so please make sure the IED is always powered on before you get the reover password, and make sure you input the recover password within 120 hours.

2.1.5.2 Entry of the Recovery Password

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 is done at the local front panel and it causes the IED to reset the RBAC back to default.

On this action, the following message is displayed on the front panel of the IED:

```
RBAC reset done
Press any key
```

2.1.6 Port Disabling (Equipment Hardening)

The availability of unused ports could provide a security risk. Hence, unused ports can be disabled (also known as equipment hardening) – either via the front panel or by Easergy Studio software. An Engineer role is needed to perform this action.

These physical ports and logical ports can be enabled/disabled:

Port Types	Menu Text	Col	Row	Default Setting	Available Value
Physical Ports	Front Port	25	05	Enable	Enable/Disable
	Rear Port 1	25	06	Enable	Enable/Disable
	Rear Port 2	25	07	Enable	Enable/Disable
	Ethernet Port 1	25	08	Enable	Enable/Disable
	Ethernet Port 1/2	25	09	Enable	Enable/Disable
	Ethernet Port 2/3	25	0A	Enable	Enable/Disable
	Ethernet Port 3	25	0B	Enable	Enable/Disable
Logical Ports	Courier Tunnel	25	0C	Enable	Enable/Disable
	IEC61850	25	0D	Enable	Enable/Disable
	DNP3oE	25	0E	Enable	Enable/Disable

Table 10 - Port hardening settings

Note
The port disabling setting cells are not provided in the settings file. In addition, it is not possible to disable simultaneously more than one physical port or Logical port. New redundant Ethernet boards have three physical ports but total two interfaces. The actual disabled physical port is depended on the redundant communication mode (PRP, HSR, RSTP or Dual IP). Refer to the Dual Redundant Ethernet Board (Upgrade) (DREB) chapter (Px4x/EN EB) for more details.

When the Ethernet board related physical ports or logical ports are disabled or enabled, the Ethernet card will reboot. The status of the ports will be available after reboot of the Ethernet board.

For more details about how to disable/enable the unused ports, please see sections:

- 3.3 - How to Disable a Physical Port
- 3.4 - How to Disable a Logical Port

2.1.7 Security Logs

The Security Logs need to store logs from each item of equipment. These logs are generated by the system, and cannot be edited by the user. A variety of different items are recorded, including: bad/faulty access attempts, login attempts, authentication errors, changes to roles, users and access control lists, network backup and configuration changes, communication failures and so on.

Security logs emissions depend on the security standards that are configurable by the SAT.

The security logs will push to a Syslog server if the Syslog server IP address and Syslog server IP port are configured and connected.

SAT also can be used to explore the security logs but Easergy studio is not supported.

The settings for the security log standards and Syslog server IP address and ports are listed in the Configurable cyber security settings table. For more detail about the security log configuration, please refer to the SAT documentation.

> Note
> The Security logs time stamp may be time shifted by several milliseconds compared with local event log. The security logs will not be generated if the Ethernet card is starting up. If the Syslog server is unavailable, the new logs will be stored and overwriting the oldest logs.

This table lists the security logs categories available for each standard.

Log ID	Additional field	Explanation	Level	Standards					
				BDEW	E3	NERC CIP	IEEE 1686	IEC 62351	CS Phase 1
CONNECTION_ SUCCESS	The additional field will contain the issuer of the connection: LOCAL or NETWORK	Successful connection	INFO	x	x	x	x		x
CONNECTION_ FAILURE		Failed connection (wrong credentials)	WARNING	x	x	x	x		x
CONNECTION_ FAILURE_ AND_ BLOCK		Failed connection (wrong credentials) triggering the blocking of the account on the IED	DANGER	x	x	x	x		x
CONNECTION_ FAILURE_ ALREADY_ BLOCKED		Failed connection because of a blocked userID on this IED	DANGER	x	x	x	x		x
DISCONNECTION		Disconnection triggered by the peer /user	INFO	x	x	x	x		x
DISCONNECTION_ TIMEOUT		Disconnection triggered by a timeout	INFO	x	x	x	x		x
CONTROL_ OPERATION	Type & Data associated to the control	Trace and control / override of real data from a peer	INFO				x		
CONFIGURATION_ DOWNLOAD	Version	Download of the configuration file from the device - Files include PSL, Courier setting, DNP setting,	INFO				x		

Log ID	Additional field	Explanation	Level	Standards					
				BDEW	E3	NERC CIP	IEEE 1686	IEC 62351	CS Phase 1
		MCL/CID and user curves (crv)							
CONFIGURATION_ UPLOAD	Version	Upload of a new configuration file into the device - Files include PSL, Courier setting, DNP setting, MCL and user curves (crv)	INFO				x		
RBAC_UPDATE	Version	Update of the RBAC cache in the IED	INFO				x		x
SEC_LOGS_ RETRIEVAL	Version	Retrieval of the security logs of the IED	INFO				x		
TIME_CHANGE	New & Old time	Modification of the time of the IED	INFO				x		
REBOOT_ORDER	None	Reboot order sent to the IED / IED start up	DANGER				x		x
PORT_ MANAGEMENT	Port, action (enable / disable)	Any comms port enabled / disabled	INFO						x
AUTHORIZATION_ REQ	Action, object	Any authorization request sent to the CS brick	INFO			x		x	x

Table 11 - Security logs recorded

2.1.8 Common Cyber Security Settings

The System Administrator can customize the cyber security settings at the SAT. The following table shows the common cyber security settings. Parts of settings also are visible on the IED with specific Courier cells but not editable in IED or Easergy Studio. These are shown in the right-hand columns of this table:

Setting in SAT	Default Setting	Available Value	Menu in IED	Col	Row
Minimum inactivity period	15	1 to 99 Minutes	-	-	-
If the user does not perform any action within this interval, the user will be logged off.					
Allow user locking	Yes	Yes/No	-	-	-
Option allows user account locking					
Maximum login attempts	5	1 to 99	Attempts Limit	25	02
The maximum failed password entry attempts, the user will lock once the attempts reached.					
Password attempts timer	3	1 to 30 Minutes	Attempts timer	25	03
The time for reset the attempts count to 0. The user got to maximum login attempts.					
Automatic user account unlocking	Yes	Yes/No	-	-	-

Setting in SAT	Default Setting	Available Value	Menu in IED	Col	Row
Enable/disable the attempts times aromatic reset function.					
Locking period duration	240	1 to 86400 Seconds	Blocking timer	25	04
The Locking period duration (seconds)					
Password Complexity	None	None / IEEE1686/ NERC	-	-	-
Set the password compliant standard.					
Log and monitoring standard	BDEW	BDEW / E3 /NERC-CIP / IEE1686 / IEC62351/ CS_PH1	-	-	-
Setup security log emission standard					
Syslog server IP address	0.0.0.0		-	-	-
Syslog server IP address					
Syslog server IP port	601	1 to 65535	-	-	-
Syslog server IP port					

Table 12 - Configurable cyber security settings

These settings show some common information about cyber security, which are not configurable whether by SAT, or Easergy Studio or the front panel.

Menu in IED	Col	Row	Description
User Banner	25	01	Show user banner information: ACCESS ONLY FOR AUTHORITY USERS.
Attempts remain	25	11	Show the remains attempt times for user login
Blk time remain	25	12	Show the remains time for blocked user to unlock
User Name	25	21-2F	Configured user name (in SAT)
Security Code	25	FE	The security code used to recovery the password.
RBAC Password	25	FF	Enter 16 characters recover password to recovery password

Table 13 - Un-configurable cyber security settings

2.1.9 Local Default Access

Local Default Access function can be disabled/enabled in the SAT.

The intention for Local Default Access function is to allow the user easy to access the IED from the front panel and without any authorization required. This means if the Local Default Access function is enabled, everyone will be authorized to access the front panel with associated Rights.

By default, the Local Default Access has the VIEWER role, it is also possible to associate the other Roles to the Local Default Access, which is configurable in the SAT.

Local Default Access function is only available in the front panel.

The Local Default Access login/logout process is invisible for the user.

2.2 MiCOM Px4x with CSL0 - Simple Password Management

For MiCOM Px4x IED with CSL0, as the Security Administration Tool (SAT) is not supported, all the cyber security features which need SAT support will not be available.

This section describes the different implementations by comparing with CLS1.

The cyber security features that are not mentioned in this section will default to be the same as CSL1.

2.2.1 Password Management

For MiCOM Px4x IED with CSL0, SAT is not supported for the configuration, so only the alphanumeric password can be used.

- The alphanumeric password is settable via Easergy Studio and the Front panel
- Passwords may be any length between 1 and 16 characters long
- Passwords may contain any ASCII character in the range ASCII code 33 (21 Hex) to ASCII code 122 (7A Hex) inclusive
- No password compliance is required
- The alphanumeric password will used for Courier access and the front panel access

Arrow key password is not available for IED with CLS0.

Important
The Schneider Electric password policy is one of the key elements of the Cyber Security Policy.
Good practice to improve the Password definition:
- Use common Cyber Security Good Practice for password complexity definition by using strong passwords.
- Change All Passwords from their default value when taking the protection device into use. (User must change password after first login).
- Change Passwords regularly. (User must update password after a certain period of time).
- Use NERC Compliant password as much as possible.
- Enforce the use of strong and complexes Password as : Caps characters + Lowercases characters + Numbers + Special characters in one password.
- Set the minimum password length to 10 characters.
- Switch off all Comm port not use on the device, if possible.
- Do not reuse old passwords.
- All P40 relays installed before January 2020 should be checked separately case by case to confirm the Cyber Security conformity to Standard/country law.
All user must be aware of best practice concerning passwords, these include:
- Not Sharing personal passwords.
- Not displaying passwords during password entry.
- Not transmitting passwords in email or by other means.
- Not saving the passwords on PC's or other devices.
- Not written password on any supports.
- Regularly reminding users about best practices concerning password.

2.2.2 Fixed Factory RBAC

For MiCOM Px4x IED with CSL0, the user list and its role/right will be fixed as factory RBAC and not configurable. Refer to the *Factory RBAC* table for more details.

2.2.3 Security Logs Service

The security logs services are not available for MiCOM Px4x IED with CSL0.

2.2.4 Cyber Security Settings

For MiCOM Px4x IED with CSL0, all cyber security settings are fixed as default setting and un-configurable. Refer to the *Configurable cyber security settings* table for the default settings.

2.2.5 Disable/Blank Password

For MiCOM Px4x IED with CSL0, it is possible to remove the user password. In MiCOM S1 Studio, this is achieved by click the BOX "Disable the password". In the IED, this is achieved

by setting the password as blank.

Once the password is disabled/blank, the user can login to the IED directly and there is no need to enter the password.

3. HOW TO USE CYBER SECURITY FEATURES

These 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.

3.1 How to Login

3.1.1 Local Default Access

If the Local Default Access is enabled, the user may login to the front panel with associated roles.

3.1.2 Auto Login

Auto login means the user will login the IED automatically and no need to select the user name and enter the password. In this case, the user will be authorized with relevant rights. The auto login will be applied in these cases:

CS Version	Interface	RBAC/PW Cases	Login Process
CSL1	Front panel	Factory RBAC	Auto login with **EngineerLevel**
		Customized RBAC	Local Default Access Enabled: Login with **Local Default Access** Local Default Access Disabled: Login with **Prompt User List**
	Courier Interface	All cases	Login with **Prompt User List**
CSL0	Front panel	Factory RBAC	Auto login with **EngineerLevel**
		Password changed	**EngineerLevel** password is “AAAA” or is disabled/blank: Auto login with **EngineerLevel**. **OperatorLevel** password is “AAAA” or is disabled/blank: Auto login with **OperatorLevel**. **EngineerLevel** and OperatorLevel password changed: Auto login with **ViewerLevel Access**
	Courier Interface	Factory RBAC	Auto login with **EngineerLevel**
		Password changed	**EngineerLevel** password is “AAAA” or is disabled/blank: Auto login with **EngineerLevel**. **OperatorLevel** password is “AAAA” or is disabled/blank: Auto login with **OperatorLevel**. **EngineerLevel** and **OperatorLevel** password changed: Login with **Prompt User List**

Table 14 - Auto Login process

For more details about the Factory RBAC, please refer to the 2.1.2 - RBAC Management (via the SAT) section.

3.1.3 Login with Prompt User List

This login process will happen if:

- The Auto login process is not applied.
- Or high authorization is required for the current operation.

In this case, the IED will prompt the user list, and the user needs to select proper user name and enter the password to login.

3.2 How to Logout

3.2.1 How to Logout at the IED

For security consideration, it would be better to “logout' the IED once the configuration done. You can do this by going up to the default display. When you are at the default display and you press the ‘Cancel’ button, you may be prompted to log out with the following display:

```
ENTER TO LOGOUT
CLEAR TO CANCEL
```

You will be asked this question if you are logged in.

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

```
LOGGED OUT
UserName
```

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

```
LOGOUT_CANCELLED
UserName
```

Note
The MiCOM IED runs a timer, which logs the user out after a period of inactivity. For more details, refer to the Inactivity Timer section.

3.2.2 How to Logout at Easergy Studio

- Right-click on the device name and select Log Off.
- In the Log Off confirmation dialog click Yes.

3.3 How to Disable a Physical Port

Using Easergy Studio or the front panel it is possible to disable unused physical ports. This can not be done by the SAT. By default, 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:

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

There are between two and four ports eligible for disablement:

- Front port
- Rear port 1
- Rear port 2 (available in the specific models)
- Ethernet port (available in the specific models)

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

3.4 How to Disable a Logical Port

Using Easergy Studio or the front panel it is possible to disable unused logical ports. This can’t be done by the SAT. An Engineer-role is needed to perform this action.

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.

These protocols can be disabled:

- IEC61850 (available in the specific models)
- Courier Tunnelling (available in the specific models)
- IEC61850 + DNPoE (available in the specific models)

3.5 How to Secure a Function Key (when available)

In cyber security implementation, this function has been linked to the front panel authorization.

- When the function key pressed, if there is no user login in the front panel or the logged-in user is not authorized, a prompt message will be raised in the front panel to ask the user to login. Once the user is logged-in, they need to press the function key again to execute the command.
- If the user is already logged in and the authorization is OK, the command will be executed immediately.
- By default, the OPERATOR or ENGINEER Roles are able to operate the function keys.
- The function key will be executed immediately if the auto login process is applied and the user is authorized.
- If unauthorized users press the Function Key during the setting change, they need to commit the changes first then login with authorized user to operate the function key.

4. GLOSSARY FOR CYBER SECURITY

Term	Meaning
CIP Standards	Critical Infrastructure Protection standards. NERC CIP standards have been given the force of law by the Federal Energy Regulatory Commission (FERC)
DCS	Distributed Control System
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)
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.
MIB	Management Information Base
NERC	North American Electric Reliability Corporation
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.
SAM	Security Administration Module. Device in charge of security management on an IP-over-Ethernet network.
SAT	Security Administration Tool TSF based application used to define and create security configuration
Secured IED	Devices embedding security mechanisms defined in the security architecture document
Security Administrator	A user of the system granted to manage its security
TAT	Transfer Administration Tool
Unsecured IED	Relay/IEDs with no security mechanisms.

Table 15 - Glossary for cyber security