Table 36 - Roles vs. their access rights (Continued)

	VIEWER	OPERATOR	ENGINEER	INSTALLER	SECADM	SECAUD
Debug application				■		
Secure communication	■	■	■	■		
Device cybersecurity data full access				■		
Backup memory copy				■		
Device user data file read		■		■		
Device user data file full access				■		
Device system data file full access				■		
Function key control		■	■	■		
Setting change			■	■		
Firmware update				■		
Firmware verify				■		
Zigbee sensors pairing				■		
Zigbee board firmware update				■		
EOS-BM100 firmware update				■		

Please find detailed explanation of the rights from following table.

Table 37 - List of rights

Right	Name of right in CAE[45]	Description
Logs	LOGS	Permission to retrieve security logs from PowerLogic P5 with CAE
Debug application	P5_RightApplicationDebug	Permission to execute firmware (application level) debug command (internal manufacturer user)
Backup memory copy	P5_RightBackupRootDirDefaultAccess	Permission to read, write, delete, transfer through SFTP, back up memory data in /backup/ directory of file system embedded in the device.
Configuration read	P5_RightConfigDft	Permission to read the configuration which need a reboot of the device, for example, scaling values like CT ratio or voltage connection mode.
Configuration change	P5_RightConfigMgt	Permission to modify the configuration, it means we can change any setting which need a reboot of the device, for example, scaling values like CT ratio or voltage connection mode.
Control status read	P5_RightCtrlObjDft	Permission to read the status of controllable objects such as status of switches, alarms, digital inputs/outputs, LED mode, etc.
Control	P5_RightCtrlObjMgt	Permission to change the status of controllable objects such as switches, alarms, digital inputs/outputs, LED mode, etc.
Device cybersecurity data full access	P5_RightCybSecRootDirDefaultAccess	Permission to read, write, delete, transfer through CAE, cybersecurity data in /cyb_sec/ directory of file system embedded in the device.
Read data	P5_RightDataDft	Permission to read all the data (i.e., measurements, fixed parameters (i.e. model number, ….), logs, …
Internal data	P5_RightDescMgt	Permission to read and write internal data (internal manufacturer user)
Firmware update	P5_RightFirmwareProgram	Permission to update firmware
Firmware verify	P5_RightFirmwareVerify	Permission to verify firmware authenticity and integrity before updating the firmware to the device
Function key 1-8 control	P5_RightFnkey01-07	Permission to operate with the function keys. There is one permission per function key Fx (x = 1 to 7)

45. The name of right in CAE is needed when the rights will be assigned for new roles or to be customized for existing roles.

Table 37 - List of rights (Continued)

Right	Name of right in CAE[46]	Description
Secure communication	P5_RightSecureComm	Permission to connect eSetup Easergy Pro to PowerLogic P5
Settings read	P5_RightSettingDft	Permission to read any setting which do not need a reboot of the device, for example, protection threshold or operation time.
Settings change	P5_RightSettingMgt	Permission to modify any setting which does not need a reboot of the device, for example, protection or communication settings. Includes also logic and Mimic configuration in eSetup Easergy Pro, switching device mode (normal use or tests mode) and allowing test execution.
Read statistics data	P5_RightStatDft	Permission to read only statistics data like counters, demand, max, min., thermal capacity, …, etc.
Clear statistics data	P5_RightStatMgt	Permission to read and clear statistics data like counters, demand, max, min., thermal level, …, etc.
Debug system	P5_RightSystemDebug	Permission to execute firmware (low level) debug command (internal manufacturer user)
Device user data file read	P5_RightUserRootDirDefaultAccess	Permission to read through SFTP or eSetup Easergy Pro, user data in /usr/ directory of file system embedded in the device like disturbance records, …, etc.
Device user data file full access	P5_RightUserRootDirFullAccess	Permission to read, write, delete, transfer through SFTP or eSetup Easergy Pro, user data in /usr/ directory of file system embedded in the device like disturbance records, …, etc., except security logs.
Device system data file full access	P5_RightUserRootDirFullAccess	Permission to read, write, delete, transfer through SFTP, system data in /sys/ directory of file system embedded in the device (internal manufacturer user); permission to update, through eSetup Easergy Pro and the device firmware.
Security	SECURITY	Permission to change security settings including RBAC, password complexity, and timeout options…, etc.

Password complexity

The following rule of password complexity is available for both Basic CS level and Advanced CS level.

- Length of password must be 1 to 8 characters
- Passwords can be composed by the following ASCII [33 to 122] characters:
  - Latin capital letters from A to Z
  - Latin lowercase characters from a to z
  - Figures from 0 to 9
  - Non-alphabetic characters: [\ ] ^ _ ’ ! “ # $ %` & ‘ ( ) * + , - . / : ; < = > ? @

  NOTE: Passwords cannot contain the user account name or parts (no more than two consecutive characters) of the user's full name. To help to secure the PowerLogic P5 protection relay, the password should be as long as possible, mixing lowercase and uppercase characters, figures and non-alphabetic characters.

It is possible to configure password with CAE according to NERC and IEEE 1686 standard recommendations.

Standard	Configuration
NERC	8 characters minimum with ASCII [33 to 122] characters. The lesser of three or more different types of characters (e.g., uppercase alphabetic, lowercase alphabetic, numeric from 0 to 9, non-alphabetic characters)
IEEE std1686	8 characters minimum with ASCII [33 to 122] characters 1 lowercase letter, 1 uppercase letter, 1 digit from 0 to 9 and 1 non-alphabetic character

46. The name of right in CAE is needed when the rights will be assigned for new roles or to be customized for existing roles.

Password reset and factory reset

Starts from the firmware V02.501.101, the PowerLogic P5 protection relay supports password reset or factory reset. The solution depends on the cybersecurity level set to the device:

- For Basic Cybersecurity level, the reset will be only of the password, the settings will be kept.
- For Advanced Cybersecurity level, the reset will execute a factory reset of the device.

For Advanced Cybersecurity level, the reset can be disabled, however, the reset cannot be disabled for Basic Cybersecurity level. The available functions are summarised in the following table:

Type of reset	Basic CS level	Advanced CS level
Password reset	Yes	No
Factory reset	No	Yes
Reset can be disabled	No	Yes, INSTALLER rights is required. The default setting is "No".

Both password reset and factory reset are operated on local HMI of PowerLogic P5, under condition of having physical access to the device.

The cybersecurity level of the device is displayed at the upper right corner of the local HMI.  stands for the Basic Cybersecurity level,  stands for the Advanced Cybersecurity level.

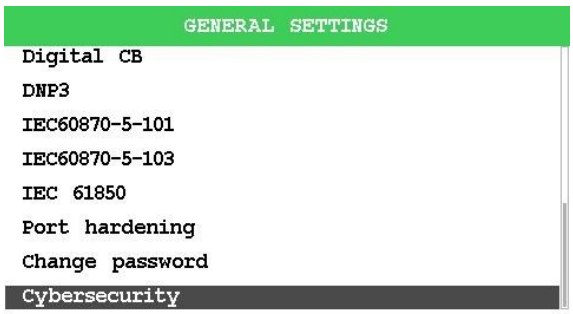
The applied solution is different with the firmware versions prior to V02.501.101, please consult related documentation or contact Schneider Electric Customer Care Centre.

Figure 160 - Padlock icons standing for the cybersecurity levels

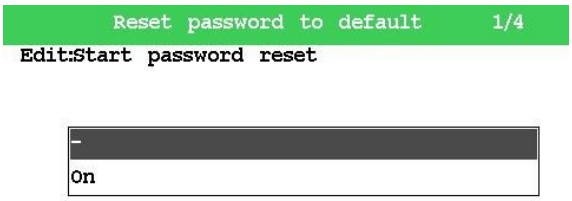
Basic Cybersecurity level: password reset

When the PowerLogic P5 with Basic Cybersecurity level is in operation mode, the password reset can be made on the local HMI:

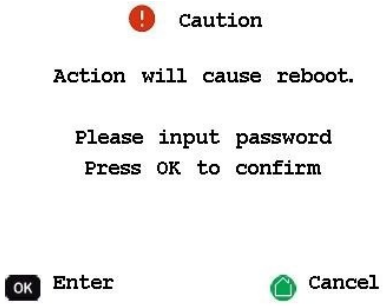
1. From the **main menu**, move the focus to **General**, then press the OK key to enter the submenu.
2. Select **Cybersecurity** option and press the OK key.



3. Then on the **Reset password to default** screen, press the OK key to activate the selection bar. Since the **Start password reset** is the only selection, press again the OK key, an option window will pop-out as shown below:



4. Select **On** option and press the OK key.
A message will appear to prompt a password input.

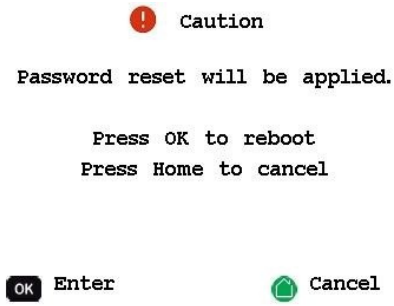


5. Press the key in sequence < ∧ > ∨ < ∧ > ∨ and press the OK key.

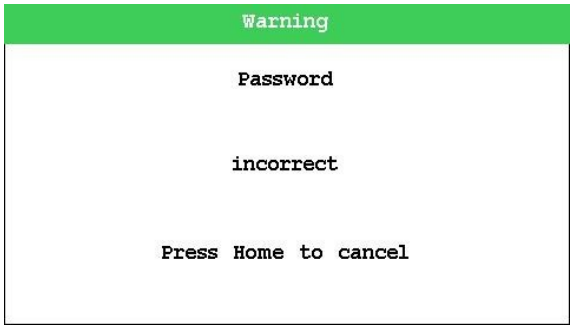
   NOTE:

   - After inputting the password (< ∧ > ∨ < ∧ > ∨), make sure press the OK key in five minutes. Otherwise the system will switch to the Mimic screen.
   - The PowerLogic P5 allows up to five attempts of password mistake. If you have reached the limitation, you will have to wait for four minutes.
   - It is recommended to short press each arrow, since there is no confirmation of the arrow pressing displayed on the screen, long pressing the arrow (more than 250 ms) can make an incorrect password input.

6. If the password is correct, a **Caution** message will be pop-outed as below. Press the OK key to reboot.



If the password is incorrect, a message will appear as shown below. Press the key to cancel and input the correct password again.

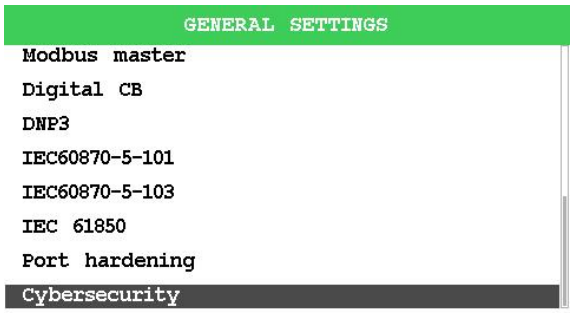


Please wait until the reboot completes.

Advanced Cybersecurity level: factory reset

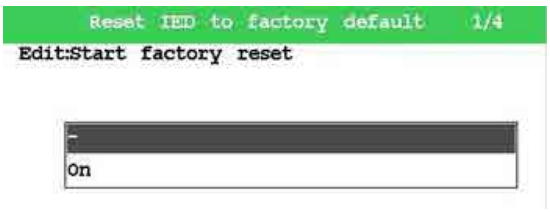
By default, **enable factory reset** setting is enabled. In case of the **enable factory reset** setting is enabled, and the PowerLogic P5 with Advanced Cybersecurity level is in operation mode, the factory reset can be made on the local HMI:

1. From the **main menu**, move the focus to **General**, then press the OK key to enter the submenu.
2. Select **Cybersecurity** option and press the OK key.

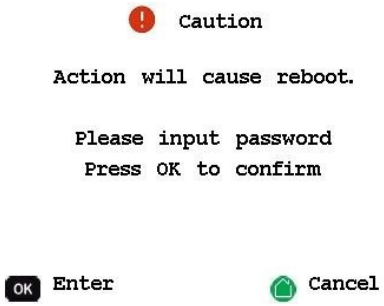


3. Then on the **Reset IED to factory default** screen, press the OK key to activate selection bar, select **Start factory reset** option.

4. Press the OK key to enter the edit page.



5. Select **On** option and press the OK key.
   A message will appear to prompt a password input.

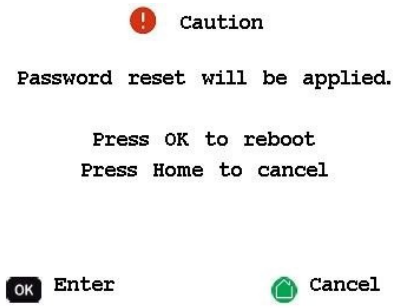


6. Press the key in sequence ◁ △ ▷ ▽ ◁ △ ▷ ▽ and press the OK key.

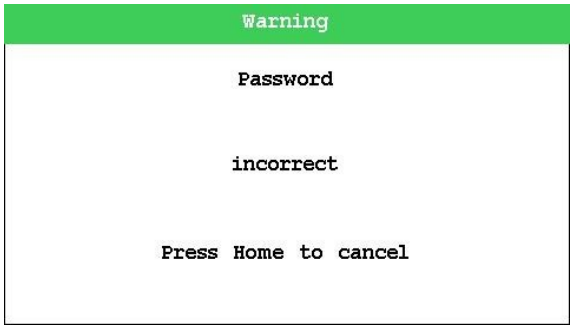
   NOTE:

   - After inputting the password (◁ △ ▷ ▽ ◁ △ ▷ ▽), make sure press the OK key in five minutes. Otherwise the system will switch to the Mimic screen.
   - The PowerLogic P5 allows up to five attempts of password mistake. If you have reached the limitation, you will have to wait for four minutes.
   - It is recommended to short press each arrow, since there is no confirmation of the arrow pressing displayed on the screen, long pressing the arrow (more than 250 ms) can make an incorrect password input.

7. If the password is correct, a message will appear as below. Press the OK key to reboot.



If the password is incorrect, a message will appear as below. Press the key to cancel and input the correct password again.



Please wait until the reboot completes. All the settings, passwords, logs and disturbance records will be reset to default values.

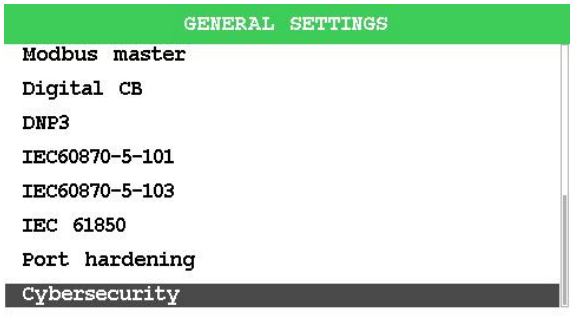
Advanced Cybersecurity level: disable the factory reset

Only the INSTALLER users are permitted to disable the factory reset by setting the **Enable factory reset** to *Off*.

NOTE: Once the factory reset is disabled, in case of the user's credentials lost, it will be impossible to perform a factory reset from PowerLogic P5 local HMI, please contact with Schneider Electric to get the technical support.

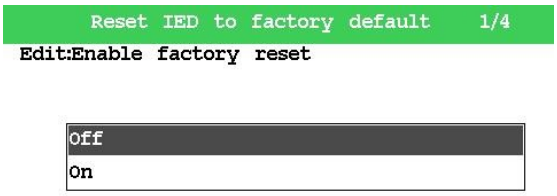
The operations to disable the factory reset are:

1. From the **main menu**, move the focus to **General**, then press the OK key to enter the submenu.
2. Select **Cybersecurity** option and press the OK key.

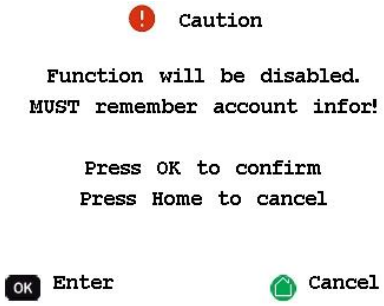


3. On **Reset IED to factory default** screen, press the OK key.

4. Press the OK key, then press the △ key to select **off**, press OK key after.



A message will appear with warning that the factory reset function will be disabled and account information must be remembered.



5. Press the OK key to confirm.
Now the **Enable factory reset** setting is set to *Off*.

Login and logout

Basic CS level comes with three fixed user accounts. Users cannot change name of those accounts. The available access interfaces for the three user accounts are as follows:

Table 38 - Accessible interfaces for user accounts of Basic CS level

User account	Role	Web HMI	Device HMI	Easergy Pro	SSH
OperatorLevel	OPERATOR	Y	Y	Y	Y
EngineerLevel	ENGINEER	Y	Y	Y	Y
InstallerLevel	INSTALLER	Y	Y	Y	Y

Advanced CS level allows user to manage user accounts and assign roles for them. The available access interfaces for roles of Advanced CS level are as follows:

Table 39 - Accessible interfaces for user accounts of Advanced CS level

Role	Web HMI	Device HMI	Easergy Pro	SSH	CAE
OPERATOR	Y	Y	Y	Y	N
ENGINEER	Y	Y	Y	Y	N
INSTALLER	Y	Y	Y	Y	N
SECAUD	Y	Y	N	N	Y (only for retrieving logs)
SECADM	N	N	N	N	Y

Login

- **Local HMI panel**: go to User Login menu from HMI main menu, then select account and enter password. Refer to Login and logout, page 248 for more information.
- **Easergy Pro software (via SSH)**: refer to Connecting to a single protection relay using USB cable, page 260 or Connecting to protection relays via Ethernet, page 260 for more information.
- **Web HMI (via HTTPS)**: Web HMI feature is disabled by default. Before use, it must be enabled in Communication menu by selecting the Ethernet port for HTTPS server. Refer to the communication user manual, search for “HTTPS server” for more information.
- **CAE (via HTTPS, only for Advanced CS level)** : only a Security Admin role (SECADM) can login to a CAE project.

Logout

For security reasons, it is recommended to logout after any operation on the PowerLogic P5 protection relay.

On the main menu screen, Login screen and Mimic screen, a padlock icon is presented at top-right corner of the title bar to signify that there is no user logged in to PowerLogic P5 protection relay. The padlock icon disappears when any user logs in.

Basic CS level setting

For Basic Cybersecurity level, the cybersecurity rules setting is straightforward:

1. The device is provided with three hardcoded account names and the names cannot be changed. Only the passwords can be changed.
2. Password change is available from the PowerLogic P5 HMI only.

Default settings

Basic Cybersecurity level comes with three fixed user accounts. CS rules are as follows:

Table 40 - Accessible interfaces for user accounts of Basic Cybersecurity level

User account	Role	Default password	Login session timeout (min)	Maximum login attempts	Password attempts timer (min)	User account locking duration (s)	Password complexity
OperatorLevel	OPERATOR	AAAA	15	5	3	240	Not required
EngineerLevel	ENGINEER	AAAA					
InstallerLevel	INSTALLER	AAAA					

The name of user account cannot be changed. The above table does not describe the rights of accounts. By default, the eSetup Easergy Pro and the P5 local HMI support maximum five consecutive failed login attempts. Once exceed the attempts, you have to wait for 240 seconds to unlock password attempts timer. The login will expire after 15 minutes of inactivity.

NOTE:

- It is strongly recommended to change default passwords of all accounts before PowerLogic P5 is put to operation.
- More information about the definition of user account parameters, refer to EcoStruxure™ Cybersecurity Admin Expert User Manual.

Changing password

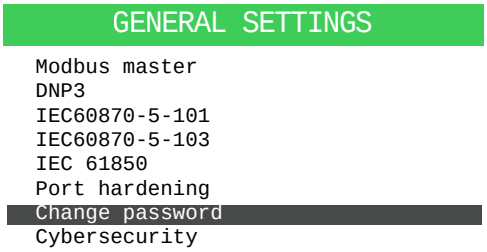
For Basic Cybersecurity level, the length of the password is 1 to 8 ASCII characters [33 to 122].

The scope of the rights of changing password for the three accounts are:

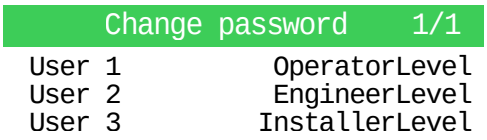
- InstallerLevel can change password for self, OperatorLevel and EngineerLevel.
- EngineerLevel can change password for self and OperatorLevel.
- OperatorLevel can change password only for self.

The password change is managed directly by the device local HMI as the following procedures:

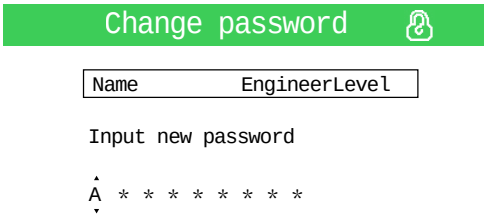
1. Login to device by entering password. If the auto-login feature is still active, then the device is already logged in with InstallerLevel account.
2. Enter the **GENERAL SETTINGS** menu and select **Change password** option.



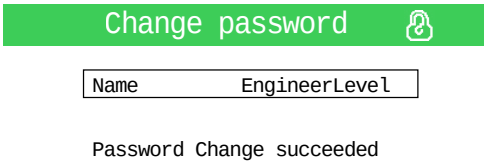
3. Select user.



4. Enter new password and then enter once again to confirm.



5. A “Password Change succeeded” message will be displayed on screen.



Special access control

Only for Basic CS level, PowerLogic P5 protection relay provides special access functions to further simplify commissioning with HMI and to enhance security:

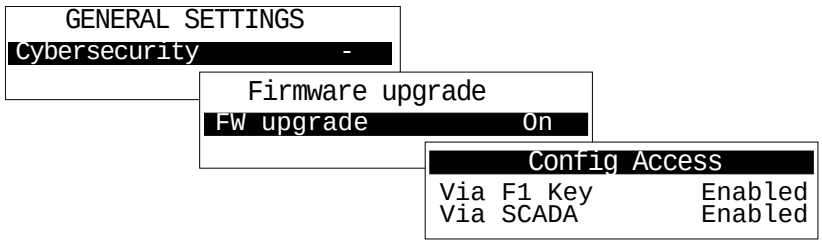
1. **Via F1 key** can be used to switch the protection relay temporarily into a mode in which the device is opened for setting change via local HMI without request of authentication.
2. **Via SCADA** can be used to switch the protection relay between local/remote modes. Therefore, once the device is set to local mode all remote setting change requests and control commands will be rejected.

PowerLogic P5 protection relay provides special access functions:

- **F1 key access control**: while “Via F1 key” disabled, F1 key works as normal function key. When “Via F1 key” is enabled. PowerLogic P5 can be switched between locked and unlocked states with F1 key. In locked state, all settings of the device become read-only, the front USB communication port is disabled, too. In unlocked state, settings of PowerLogic P5 become modifiable, settings can be modified via local panel HMI directly without username and password, front USB communication port also gets enabled. Please note that login is still required when using Easergy Pro and Web HMI in unlocked state. By setting PowerLogic P5 to unlocked state, it will bring convenience for users to configure the device during commissioning.
- **Communication SCADA access control**: the setting “Via SCADA” provides option to forbid any setting change and control command from SCADA communication protocols (Modbus, IEC61850, IEC103). If the setting is set to disabled, PowerLogic P5 rejects all SCADA protocol setting changes and control commands. However, this setting will not effect on local panel HMI, front USB communication port, eSetup Easergy Pro and Web HMI.

The settings “Via F1 Key” and “Via SCADA” can be configured from local panel HMI. This special access control is operational in Basic Cybersecurity level only.

Figure 161 - Config access Via F1 Key and Via SCADA shown on HMI



F1 key access control

PowerLogic P5 can be switched between lock/unlock states by F1 key.

NOTICE

IMPROPER EQUIPMENT OPERATION

If F1 key is configured as the quick switch of PowerLogic P5 lock/unlock, it will be not available for other functions.

Failure to follow these instructions can result in improper operation.

Table 41 - Via F1 Key configuration parameters

Via F1 Key			
	Disabled[47]	Enabled	
		Locked	Unlocked
Access via HMI	Read/Write	Read	Read/Write
Access via USB (Easergy Pro)	Read/Write	Cannot login	Read/Write
Access via rear comms (Easergy Pro)	Read/Write	Read	Read/Write
Access via rear comms (Web HMI)	Read/Write	Read	Read/Write

47. When F1 key is disabled which means it is used as a normal function key, the read/write permission is decided by existing RBAC setting.

Communication SCADA access control

For communication SCADA (Modbus, IEC 61850, IEC 103), when “Via SCADA” is disabled, setting change or control command are disabled for PowerLogic P5, whether in locked or unlocked state, with or without communication board.

Table 42 - Via SCADA configuration parameters

Via SCADA		
	Disabled	Enabled
Access via rear comms SCADA (IEC 61850)	Read	Read/Write
Access via rear comms SCADA (Modbus)	Read	Read/Write
Access via rear comms SCADA (IEC 103)	Read	Read/Write

Auto log-out

While “Via F1 Key” is enabled, PowerLogic P5 will be switched to locked state automatically in below conditions, which is called “auto log-out”:

- if PowerLogic P5 is not connected with Easergy Pro, nor with WebHMI, and without any operation on HMI for 3 minutes;
- if PowerLogic P5 is disconnected from Easergy Pro for 3 minutes;
- if PowerLogic P5 is disconnected from WebHMI for 18 minutes.

Table 43 - Login requirements and auto log-out time out

Access	Login required	Auto log-out time out		
		If without operation	If log out	If disconnected without log out
via HMI	No	3 minutes	N/A	N/A
via rear comms (Easergy Pro)	Yes	Depends on “Automatic Disconnection” setting in Easergy Pro	3 minutes	3 minutes
via rear comms (Web HMI)	Yes	Never	3 minutes	18 minutes[48]

As long as connected with Easergy Pro or WebHMI, PowerLogic P5 will not be switched to locked state.

Advanced CS level setting

With Advanced CS level, all PowerLogic P5 security rules are managed with Cybersecurity Admin Expert (CAE) software.

Please be advised that CAE offers an independent user manual which describes its function in a higher detailed level, which can be downloaded from website of Schneider Electric in more detail.

The purpose of describing CAE software in this manual is to help PowerLogic P5 users start with the Advanced CS level configuration without having to read the complete CAE user manual. For this reason, only basic operations of the software will be described. For a thorough understanding of the CAE functions, please refer to CAE user manual.

48. It is proposed to click on “Logout” button at top right of WebHMI before closing the web browser, the auto log-out will be launched in 3 minutes.

Before configuring with CAE, PowerLogic P5 device of Advanced CS level is equipped with default security settings.

Default settings

The default Advanced Cybersecurity level users of PowerLogic P5 are:

Table 44 - Accessible interfaces for user accounts of Advanced Cybersecurity level

User account	Role	Default password	Login session timeout (min)	Maximum login attempts	Password attempts timer (min)	User account locking duration (s)	Password complexity
OperatorLevel	OPERATOR	AAAA	15	5	3	240	Not required
EngineerLevel	ENGINEER	AAAA					
InstallerLevel	INSTALLER	AAAA					
SecurityAdmin	SECADM	AAAAAAAA					

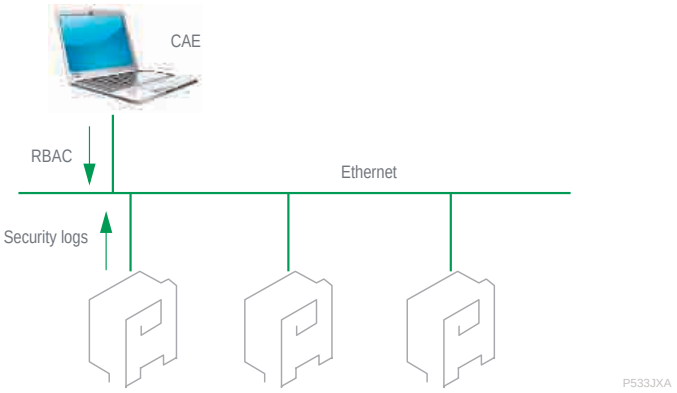
By default, the eSetup Easergy Pro and the P5 local HMI support maximum five consecutive failed login attempts. Once exceed the attempts, you have to wait for 240 seconds to unlock password attempts timer. The login will expire after 15 minutes of inactivity.

More information about the definition of user account parameters, refer to EcoStruxure™ Cybersecurity Admin Expert User Manual.

Introduction of CAE software

CAE allows users to centrally update usernames and passwords for all PowerLogic P5 devices in the same local area network without having to do it bay-by-bay. It can customize the rights of user roles and user accounts. More advanced features of CAE include configuring the Syslog server, extracting locally saved security logs from PowerLogic P5 devices, and centralized authentication over RADIUS/LDAP protocol with a Microsoft Active Directory as the back end.

NOTE: CAE projects can be only opened and edited by SECADM (Security Administrator) accounts.



System requirements

CAE is a software with no requirement of license nor cost. It can be downloaded for free from Schneider Electric's website.

CAE runs in Windows® 10 Professional version 32/64 bit.

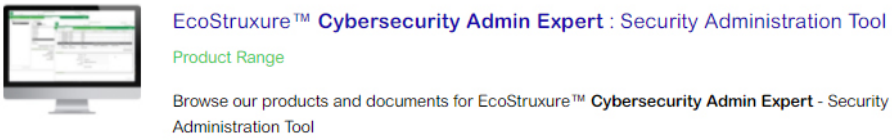
Administrator's privilege is required to install CAE application components to Windows. After installed, non-administrator users will be also able to use the software.

To connect and manage PowerLogic P5 devices with CAE, the computer with CAE shall be in the same local area network with the devices.

CAE download and install

Go to https://www.se.com/ww/en/all-products and search for Cybersecurity Admin Expert to find the product page of CAE, click to enter product page.

Figure 162 - Product page of CAE



Click **See software** to choose package between x86 and x64 versions according to operating system of the computer to install CAE. The latest version of CAE at the time when this chapter was written is 2.2.1.2304.

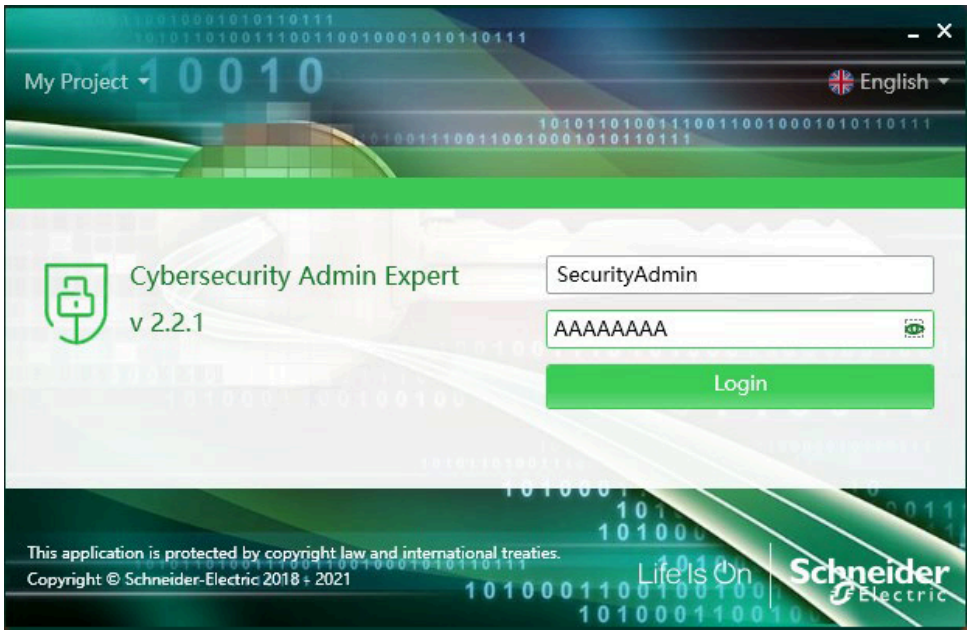
NOTE: CAE only runs in Window 10. It will not run in Windows 7.

After downloading the installation package, unzip the package and run the **Cybersecurity Admin Expert Installer.exe** file to install. The files in folder ISSetupPrerequisites will be installed automatically.

Changing initial password

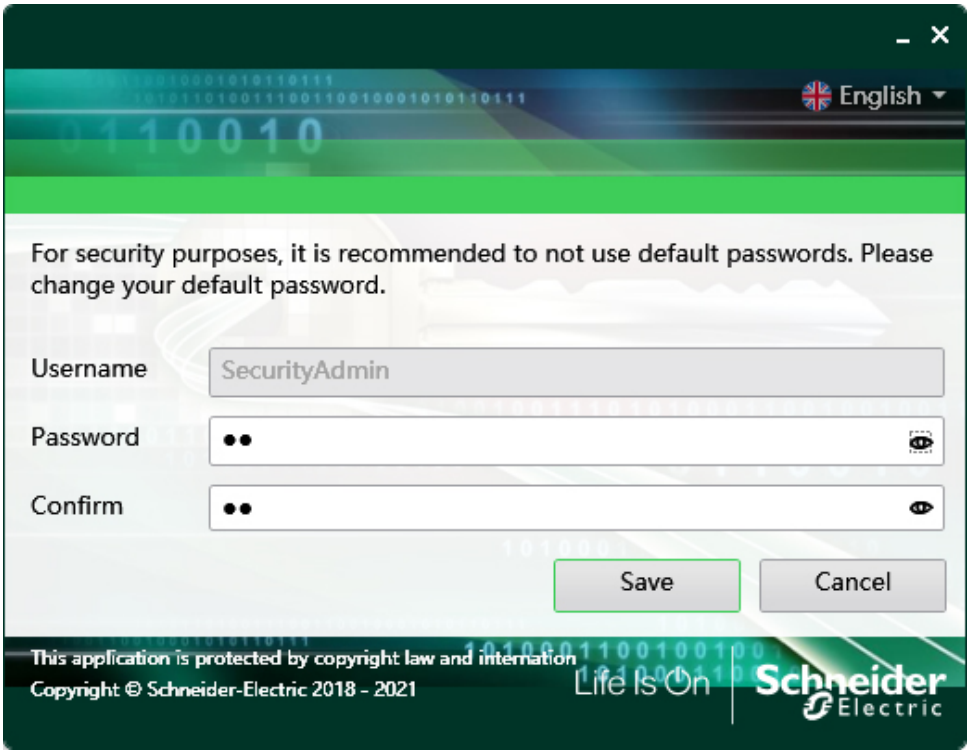
When launching CAE for the first time it will prompt for a username and password. The default username is *SecurityAdmin* with default password: AAAAAAAA. The username and password are both case sensitive.

Figure 163 - Initial password of CAE



Account will be locked if password is entered incorrectly up to 5 times. If this is the only SECADM account of a project, a few minutes of waiting is obliged before any further attempts with the same account. Alternatively, the blocked account can be unblocked with another SECADM account immediately by using it to open the project. Once the project is opened, all blocks of SECADM accounts will be cancelled immediately.

After correctly entering the default username and password, CAE will ask for the default password of the SecurityAdmin account to be changed.

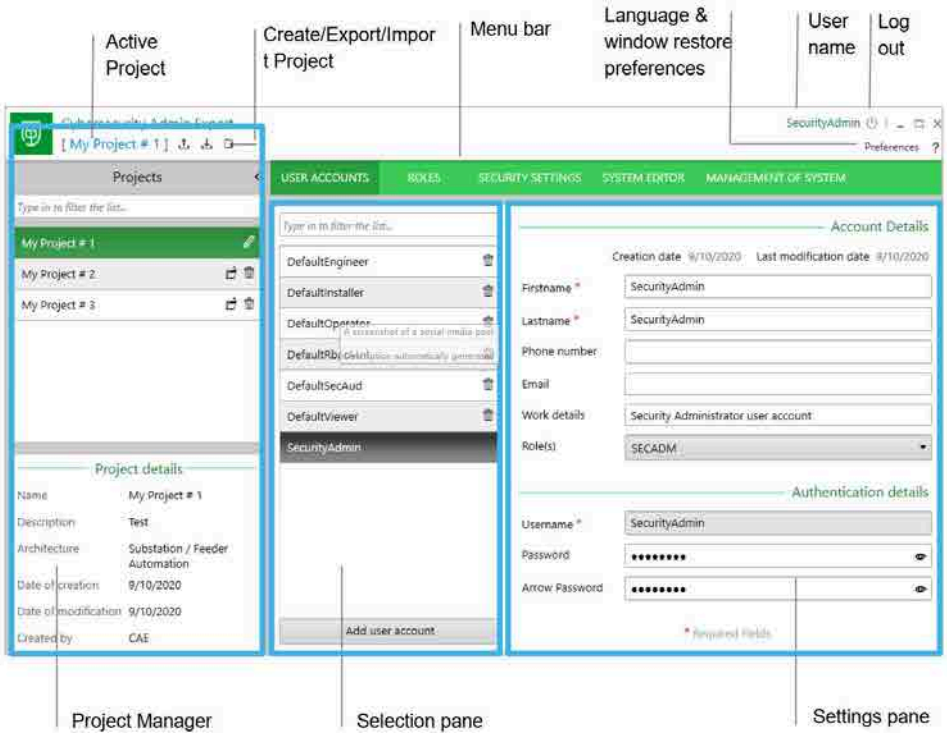


There is no password complexity requirement for a new project. When entering password input, you can click and hold the icon of eye to verify input.

CAE user interface overview

Cybersecurity Admin Expert (CAE) user interface window is composed of three main work areas:

1. Project Manager pane at left
2. Selection pane in the center
3. Settings pane at right



- **Menu Bar**: From the menu bar user can select required function. The organization of functions follows a typical configuration workflow, however, user can jump from one to another.
- **Preferences**: Click to choose language and activate/deactivate window restore preferences.
- **Username**: Logged in username is displayed in this area.
- **Log out**: To log out from the application, click on the power **on/off** icon.
- **Help**: click **?** icon then **Audit Logs** to see CAE application logs.
- **Create/Export/Import**: Use those buttons to create, export or import CAE security configuration project database.

Most of the CAE functions can be used without connection to PowerLogic P5 devices. Connection with devices in the same local area network is only required when using function of **MANAGEMENT OF SYSTEM** for pushing new CS rules to devices.

CAE functions are grouped in the following menu bars:

- **USER ACCOUNTS**: the functions for account edit such as create, rename, remove account, change password of account, and assign accounts to roles. Please note that one user account can be assigned to multiple roles. This user account will then have the rights of all corresponding roles combined.
- **ROLES**: edit PowerLogic P5 user roles and rights. User's rights are decided by the roles the user accounts are assigned to.
- **SECURITY SETTINGS**: set miscellaneous security-related features, such as session time out duration, password complexity requirement, Syslog server, account locking.
- **SYSTEM EDITOR**: list the discovered protection relays so that CAE can push new CS settings to the devices. Please note that PowerLogic P5 devices can be discovered automatically by CAE, since PowerLogic P5 supports DPWS and UDP. Therefore declaring of devices is optional. For devices that do not support UDP they must be added to the list otherwise CAE cannot find them.
- **MANAGEMENT OF SYSTEM**: discover PowerLogic P5 devices so that new CS settings can be pushed.

CAE recommended workflow

The CS rules of devices are managed with CAE by projects. Each project contains a set of roles and user accounts, with various security-related settings. The project can be worked offline, meaning there is no need to connect to PowerLogic P5 devices when changing the settings. When offline work is done, CAE can be connected to devices and push the project settings to them.

NOTE: changing CS rules with CAE is a one-direction process. It means new settings can be pushed from CAE to PowerLogic P5, but existing CS settings cannot be pushed back to CAE.

The recommended workflow with CAE for PowerLogic P5 is as follows:

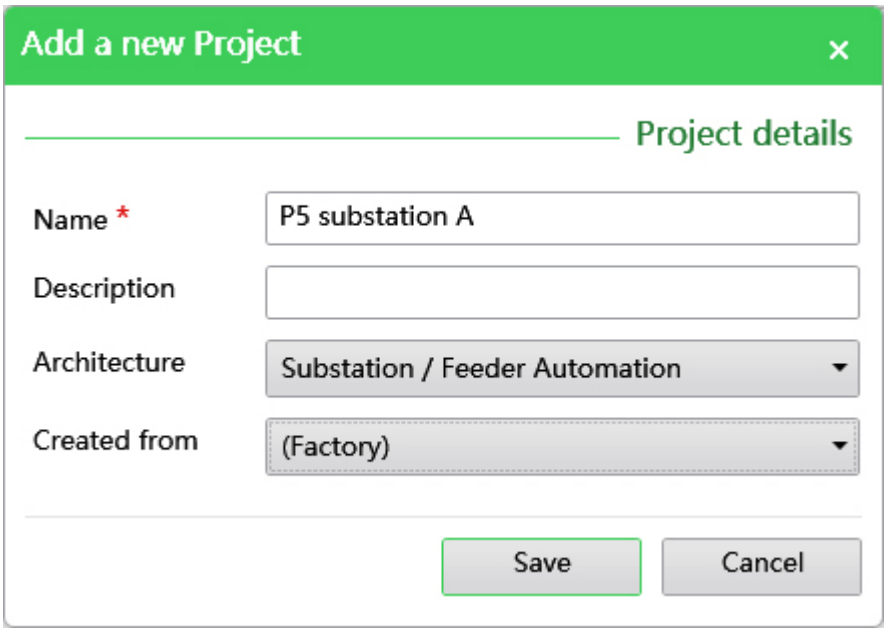
1. Manage the project: use the Project manager to open an existing CAE project or to create a new one.
2. Manage the user accounts: go to USER ACCOUNTS menu to create/remove/modify user accounts, assign roles to the accounts, and set passwords for accounts.
3. Manage the roles: go to ROLES menu to check whether the default rights of roles are in line with your organization cybersecurity policy. Rights can be changed for existing roles. New roles can be created. Existing roles can be removed.
4. Manage other security settings: go to SECURITY SETTINGS menu to set options including timeout, user account locking, password complexity, Syslog server, Security banners, and centralized authentication methods.

5. Define the devices: go to SYSTEM EDITOR to provide IP addresses of devices to CAE to let CAE connect with them. This step is optional for PowerLogic P5 because CAE can discover PowerLogic P5 devices automatically via DPWS and UDP.
6. Prepare the connection between computer with CAE and PowerLogic P5 device: CAE can connect with PowerLogic P5 through Ethernet and the front USB port. To connect through Ethernet connection make sure the computer with CAE is in the same local area network with PowerLogic P5 devices to be managed. Ensure quality of connection by USB cable if connect with front USB port. Use only one type of connection at a time.
7. Push new CS rules to PowerLogic P5: go to MANAGEMENT OF SYSTEM, use discover function to automatically find all PowerLogic P5 devices, and push new CS rules to them.

CAE menu: Projects

Click **Create a new project** button to create new project.

Example settings are as follows:



Selection in **Architecture** will impact the Security Settings menu which will be described in CAE menu: Security settings, page 220.

If the selection *Factory* is selected in **Created from** setting, the default CAE template will be used. Alternatively, it can be created from one of existing projects.

Click **Save** to save the project. Then double-click the new project in the project manager pane to switch to the project. CAE will ask for authentication upon opening the new project.

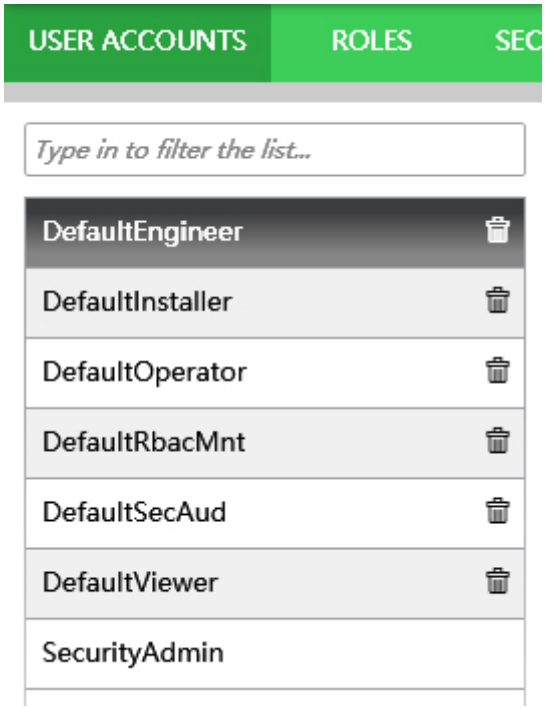
Use the account name *SecurityAdmin* and default password “AAAAAAAA” to login. CAE will then force changing of the initial password. There is no password complexity requirement for a new project.

After the password of SecurityAdmin has been changed, the project will be loaded with CAE default template settings if *Factory* is chosen to create the project from.

NOTE: CAE projects can only be opened by accounts of SECADM (Security Administrator) role.

CAE menu: User accounts

The default user accounts for any new project created from *Factory* template are as follows:



It is advised to delete the “DefaultRbacMnt” account, because this role is not supported by default in PowerLogic P5’s roles template.

New created accounts can be assigned with roles. Each account can be assigned with multiple roles. It will then get the rights of all the assigned roles combined. The “Username” is the account name which will be used for authentication.

The default alphanumeric password for all user accounts is “AAAAAAAA”.

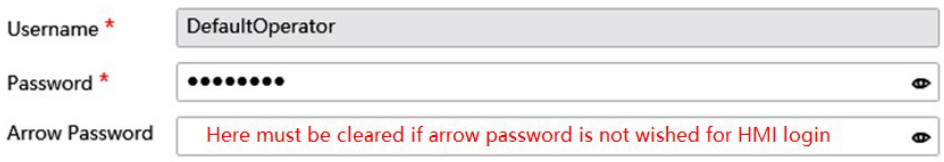
The arrow password facilitates operation of password input on the device HMI with arrow buttons.

Default passwords for all default accounts are as follows.

Table 45 - Default CAE alphanumeric and arrow passwords for PowerLogic P5

Account name	Role	Alphanumeric password	Arrow password
DefaultEngineer	ENGINEER	AAAAAAAA	↓←↑→↓←↑→ (then press OK key)
DefaultInstaller	INSTALLER		
DefaultOperator	OPERATOR		
DefaultSecAud	SECAUD		
DefaultViewer	VIEWER		
SecurityAdmin	SECADM		

If the arrow password is set in CAE, the PowerLogic P5 always prompts this authentication mode in the local HMI. If the feature is not required, please make sure to clear the arrow password for all the accounts as shown in below example.



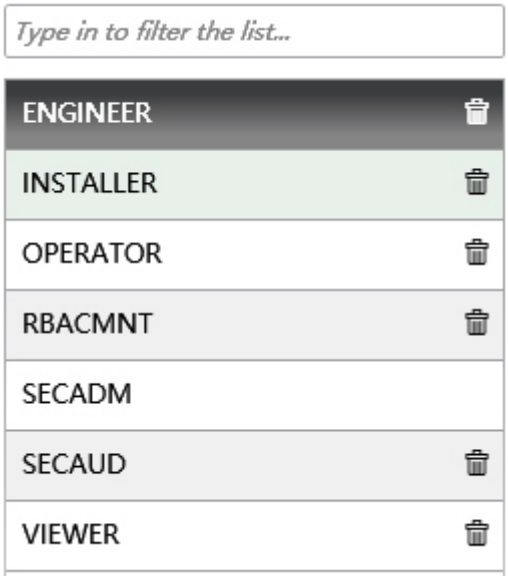
Alphanumeric password will always be asked for authentication requests from Easergy Pro and Web HMI.

NOTE:

1. It is strongly recommended to change the default passwords for all accounts before PowerLogic P5 is put to operation.
2. It is strongly recommended to create a 2nd user account assigned with SECADM role, so that in case of SecurityAdmin password lost, the 2nd SECADM account can be used to open the CAE project and recover passwords.
3. In case of managing multiple CAE projects in parallel, keep at least one SECADM account with the same password in all projects, so that to switch easily between CAE projects.
4. SecurityAdmin is the account with a hardcoded username for all CAE projects as well as for the devices. The username cannot be changed or deleted. Other roles cannot be assigned to this account (except SECADM).
5. Make sure to save changes for each account.

CAE menu: Roles

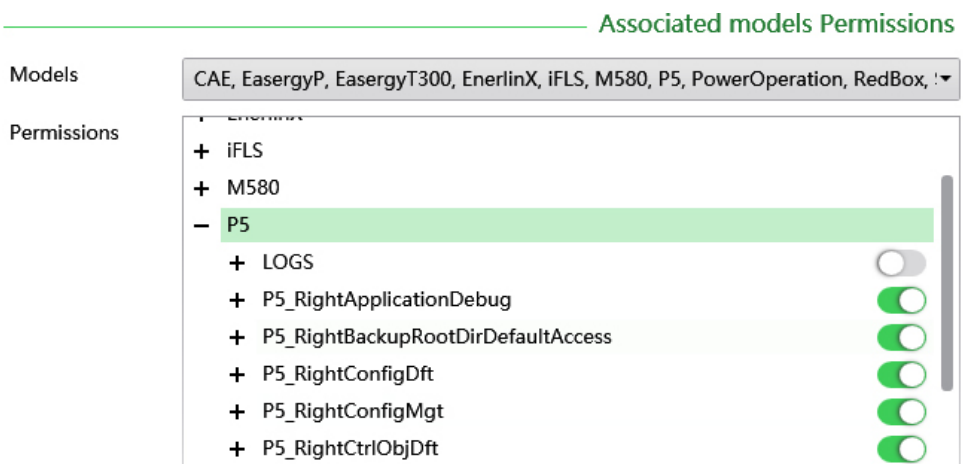
The default roles for CAE projects are as follows:



It is recommended to remove the role RBACMNT unless it is absolutely needed.

The rights of existing roles can be modified in the **Role Details** fields. Please note that CAE is designed to manage CS rules for multiple Schneider Electric products. To modify rights of PowerLogic P5, please click on the **+** sign at left of **P5** and leave the other products.

NOTE: the setting **EasergyP** is not for PowerLogic P5.



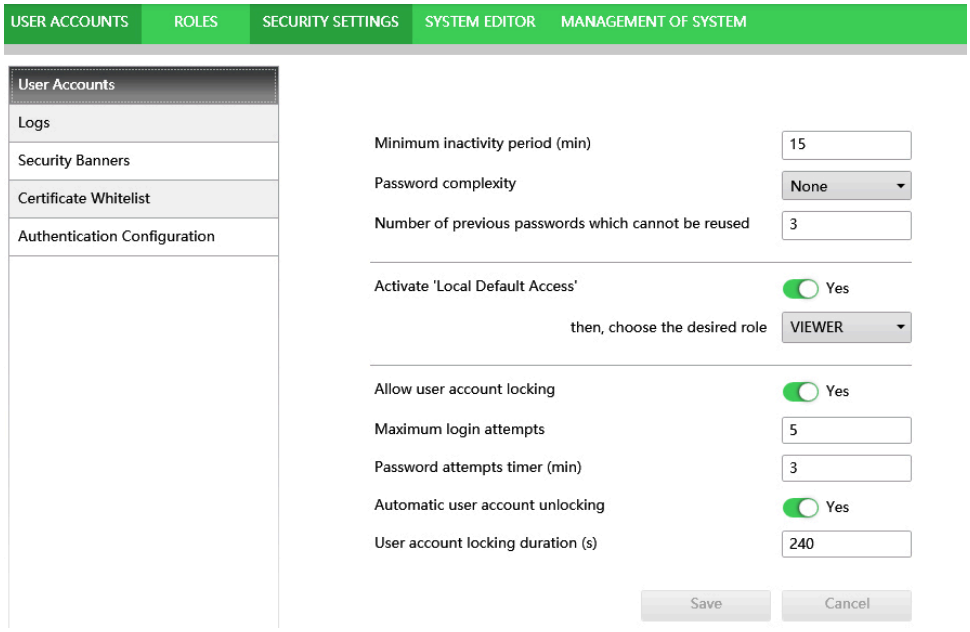
New roles can be added as needed.

CAE menu: Security settings

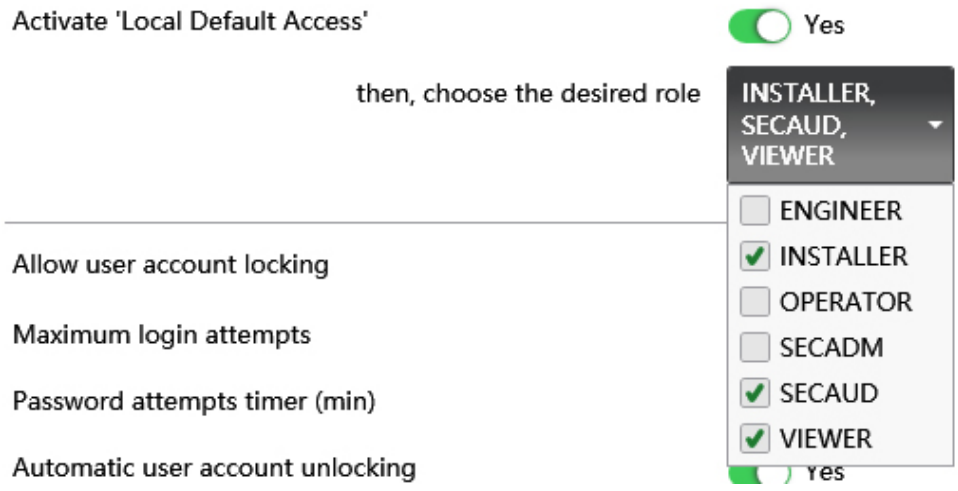
The functions in this menu make settings of various security parameters.

User Accounts

CAE is delivered with default security parameters as follows:



To facilitate operation and setting via local HMI, **Activate 'Local Default Access'** can be set to *Yes* to automatically grant selected rights of the role. Anyone who can access to the PowerLogic P5 local HMI will have the rights of the roles assigned with *'Local Default Access'*. The default setting is VIEWER, but it can be extended to multiple ROLES if needed as follows:



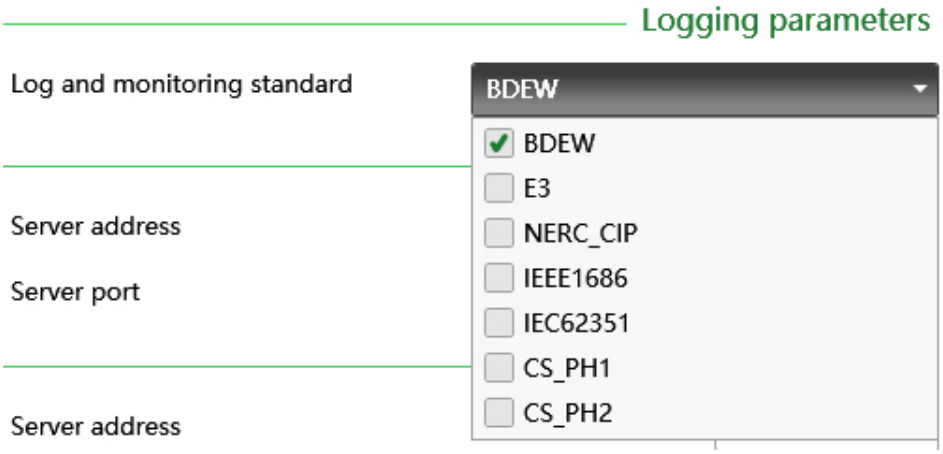
Please note that the *'Local Default Access'* option is only available for Substation / Feeder Automation architecture.

NOTE: The setting of project architecture will also impact the following options:

- **Allow user account locking**: can only be *YES* for Critical Power and Plant Automation.
- **Automatic user account unlocking**: can be only *YES* for Critical Power and Plant Automation.

Logs

- **Logging parameters**: no standard logging parameters were enabled when PowerLogic P5 was released from factory. It will not generate any security log before being managed with CAE. During creation of a new CAE project the default standard enabled by CAE is BDEW. PowerLogic P5 also supports security logs according to IEEE 1686 standards. For type of logs and which will be generated for both standards refer to Security event logging, page 234.

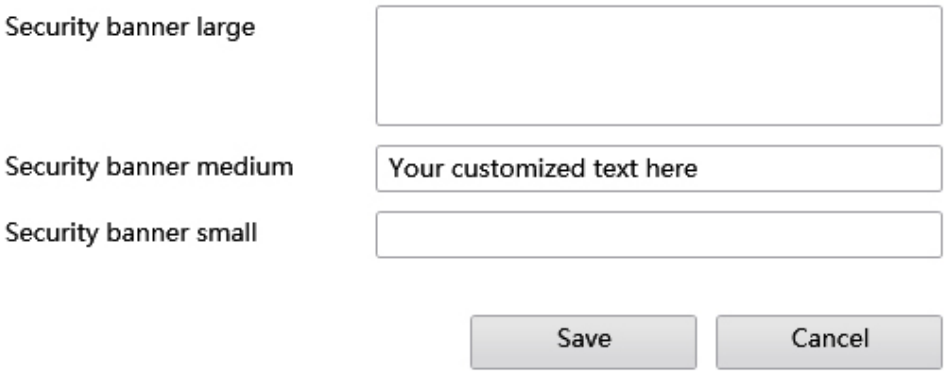


- **Syslog parameters**: input remote Syslog server address and port in this section. PowerLogic P5 will send all the internally generated security logs to the server for backup after address and port defined.
- **SNMP parameters**: the options shall not be used since PowerLogic P5 does not support SNMP.

Security Banners

The security banners are warning messages displayed on the device HMI and Web HMI login interface for system use notification.

PowerLogic P5 will display *Authorized User Access Only* before authentication takes place in the device HMI and Web HMI. The displayed message can be customized in **Security banner medium** of CAE.



Certificate whitelist

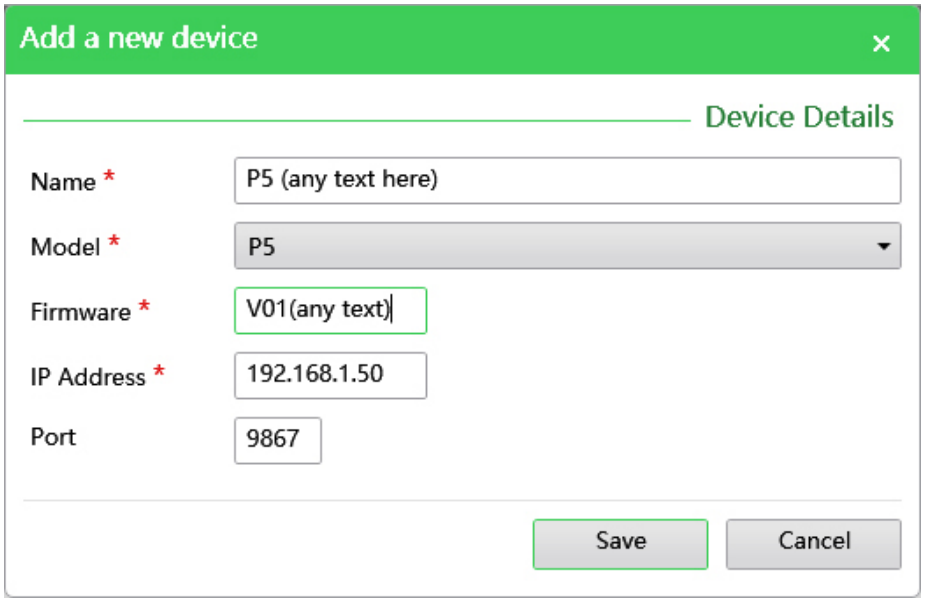
PowerLogic P5 connects with CAE via HTTPs. PowerLogic P5 works as a server with device self-signed HTTPs certificate to help ensure the credentials and contents will not be transmitted in clear text.

During network discovery period, CAE discovers a new PowerLogic P5 device and makes connection. You will be prompted to add HTTPs certificate to the white list. Verify the validity of the certificate of the device. Select it, then click **Accept** to accept a new certificate of the device.

CAE menu: System editor

This function is optional for PowerLogic P5 because CAE can discover PowerLogic P5 devices in the same local area network automatically with Advanced CS level thanks to support of DPWS and UDP protocols.

NOTE: in rare occasions CAE may not discover all PowerLogic P5 devices in same network. In this case, declaring them will help CAE find them. Specifying the **Model** and **IP Address** is sufficient, leave the **Port** by default to *9867*. The remaining of information can be free text as follows:



After making the settings, CAE should be able to find the devices.

CAE menu: Management of system

After all Cybersecurity rules have been defined, the rules will be pushed to PowerLogic P5 devices.

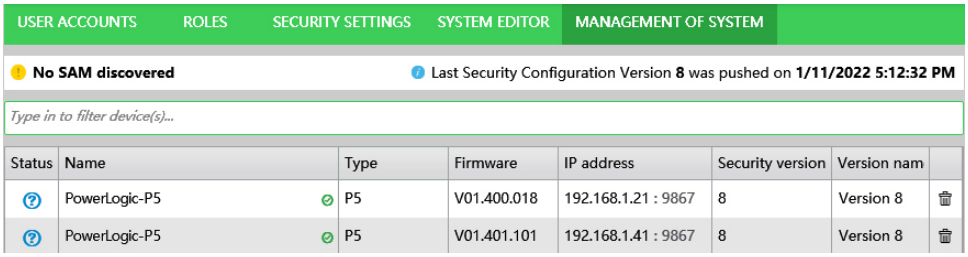
Connecting to PowerLogic P5 with CAE

CAE can connect to PowerLogic P5 via Ethernet or front USB port. To make Ethernet connection, ensure the computer with CAE is on the same local area network as the PowerLogic P5 devices to be managed. To connect through front USB port, ensure the connection quality of the USB cable between computer and PowerLogic P5.

It is recommended to use the PING command to verify the connection between PowerLogic P5 and computer with CAE when using an Ethernet connection to PowerLogic P5.

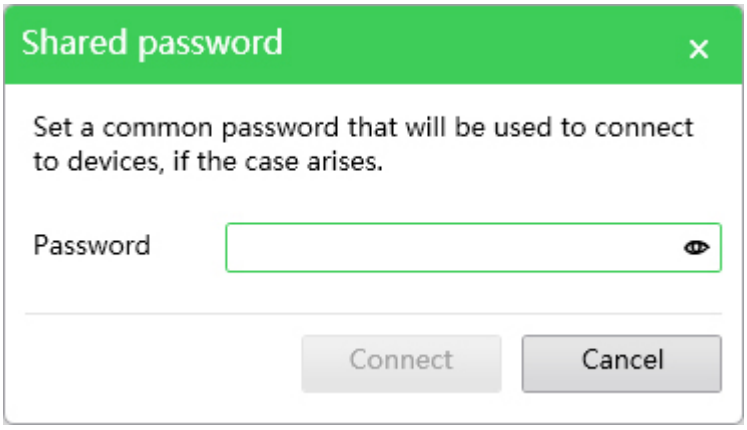
Push the new CS rules to PowerLogic P5

Click **Discover** button to find all PowerLogic P5 devices automatically in the same network as shown in image:



Click **Send security configuration** to push new CS rules to the devices.

NOTE: for PowerLogic P5 devices that have already been managed by a CAE project, the passwords of SecurityAdmin in P5 devices and the CAE project must be the same. It means if the password of SecurityAdmin of PowerLogic P5 is “ABCD”, the password of SecurityAdmin account in the CAE project must be also “ABCD”. Otherwise the user will be prompted to provide SecurityAdmin’s password. In that case the password “ABCD” must be entered to enable connection with PowerLogic P5 devices. As in image below:



As an example, if password of SecurityAdmin is changed to “EFGH”, CAE will attempt to connect with PowerLogic P5 devices with existing password “ABCD”. If it succeeds the new password “EFGH” will be pushed to PowerLogic P5 devices.

Please note that the new password and new security settings will be pushed to PowerLogic P5 devices only by clicking **Send security configuration** button again.

Retrieving PowerLogic P5 device internal security logs

Right click on PowerLogic P5 in the list of discovered devices to retrieve security logs saved internally to device. The duration of operation takes about 30 seconds.

PowerLogic P5 stores security logs in a non-volatile memory. If the memory is full, the oldest log is replaced by the newest one.

Centralized authentication

PowerLogic P5 supports centralized authentication via RADIUS and LDAP protocols, so that its user account and privilege management can be merged into an existing authentication infrastructure of the customer network. This means that the existing RADIUS server or Active Directory server in the customer network can also manage the user account and privilege for PowerLogic P5. Users can use their existing username for other devices in their network, such as other protection relays, network switches, workstations on PowerLogic P5. Once the account settings are changed at the RADIUS or LDAP server, all PowerLogic P5 devices will take account of the changes for user authentication and authorization.

Solution overview

Depending on the existing authentication mechanism used in your network, and the firmware version of the PowerLogic P5, different solutions are available:

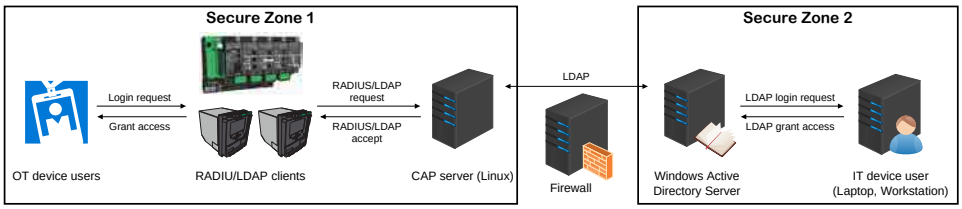
- If your existing authentication server is Microsoft Active Directory Server (referred to AD server hereinafter)
  - for the firmware version V01.500.101 and newer, you can connect to AD server directly, or with the Cybersecurity Application Platform (CAP) as a proxy. It is recommended to use the CAP as a proxy because it can simplify your firewall setup.
  - for the firmware version V01.402.201 and earlier, which only supports RADIUS, it is necessary to use the CAP as a proxy to connect to your AD server. This is because CAP can connect with the protection relay over RADIUS and connect with AD sever over LDAP.
- If your existing authentication server is RADIUS, the protection relay can be directly connected to the server
- We will use TekRADIUS as an example for connecting the protection relay and mapping the roles.

AD Server

If the existing authentication server is an AD server, it is recommended to use the CAP as a proxy to connect to the AD server. Using a CAP as a proxy can make firewall setup easier.

NOTE: The description of CAP in this document serves as a quick guide. For complete details on installing and using CAP, see the CAP documentation.

Figure 164 - Using the CAP as a proxy for connecting to the AD server

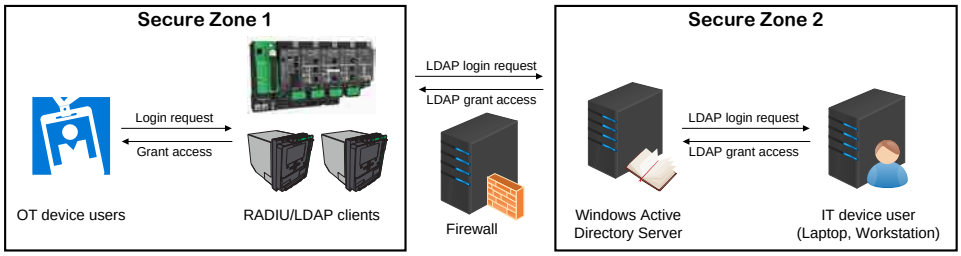


As shown above, the CAP server can be placed in Secure Zone 1 where PowerLogic P5 is located. Within the same zone there can be other devices such as RTUs, switches, and other protection relays. The firewall only needs to allow connection between the CAP server and the AD server, which makes the setup easier and more scalable.

NOTE: Secure Zone 1 is normally the most secure segment because it has OT devices which control the critical infrastructure devices such as circuit breakers and switches. Secure Zone 1 is more isolated than other network segments. Secure Zone 2 is the network used for information management services such as e-mail, file servers and Internet. Secure Zone 1 and 2 are isolated using firewalls and/or network diodes to ensure that the Secure Zone 1 is better secured.

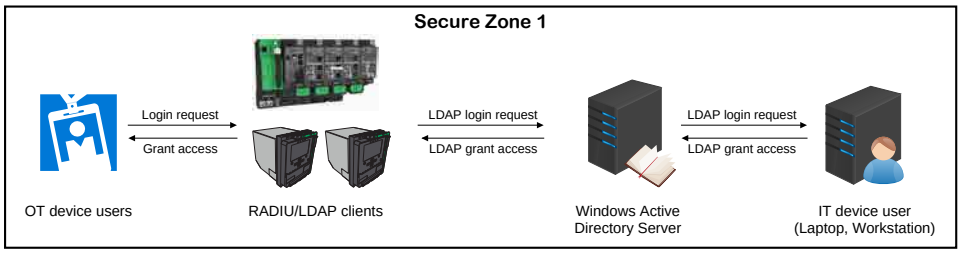
However, if using CAP is not wanted or possible, PowerLogic P5 can connect directly to the AD server with LDAP. In this case, the firewall needs to allow all PowerLogic P5 devices to connect to the AD server, as shown below.

Figure 165 - Direct connection between PowerLogic P5 and AD server, within two secure zones



Alternatively, if the AD server resides in the same Secure Zone with PowerLogic P5, there is no need to install the firewall, as shown below.

Figure 166 - Direct connection between PowerLogic P5 and AD server, within one secure zone



In the following sections, both connection methods between PowerLogic P5 and the AD server will be detailed, namely the indirect connection with CAP as the proxy, and the direct connection without CAP.

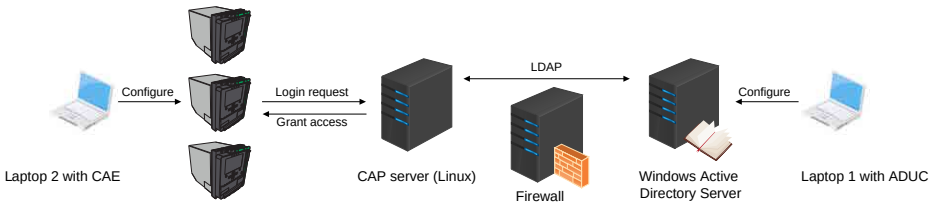
Again, it is recommended to use the CAP as the proxy if the AD server is not in the same Secure Zone as PowerLogic P5 as in Using the CAP as a proxy for connecting to the AD server, page 224.

The following items are required to carry out the configuration:

- A Microsoft Active Directory server. This is the central authentication server and the domain controller for your network. Windows Server 2019 was used when this document was written. Domain administrator privilege is required.
- A laptop with Active Directory Users and Computers (ADUC) installed. ADUC is the software to manage Active Directory objects, including users, computers, groups, organizational units (OU), and attributes. This laptop must be able to join the domain controlled by the above Windows server, for doing so the domain administrator privilege is required. This is “Laptop 1”.
- A laptop with CAE installed. With this laptop you can finish the PowerLogic P5 settings. Security Admin privilege to both the CAE project and to the PowerLogic P5 devices is required. There is no need for this laptop to join the above domain. This is “Laptop 2”. Note that you can also install CAE on your “Laptop 1” and to use only one laptop.
- A configured CAP server. For installation and configuration of the CAP server, see the CAP documentation. Administrative privilege to the CAP server is required.
- PowerLogic P5 devices in the Advanced CS mode.

When the above is all set as depicted in the following figure, the configuration can take place.

Figure 167 - Required devices and software for Indirect connection to AD server with CAP



The configuration consists of 2 or 3 steps, namely:

1. Configuration at the AD server end: this ensures that the user account is created and assigned to the user groups.
2. Configuration of the RADIUS server at the CAP end: it is only needed for older versions of PowerLogic P5. For newer versions it is not needed because LDAP can be used between PowerLogic P5 devices and the CAP.
3. Configuration at the PowerLogic P5 end: to map between user groups in the AD server and user roles in PowerLogic P5 devices.

We will use an example to walk you through.

In this example, a new user Alice WANG will be created in the AD sever. She belongs to the user group “Relay Engineer” in the domain controlled by that AD server. She should have the “ENGINEER” role privilege for the PowerLogic P5 devices.

Configuration at the AD server

In this step we will add a user and assign it to a user group in the AD server.

Use Laptop 1 to open the ADUC to connect to the AD server.

Create the user

Create a new user in the designated OU, here we use the OU “VALIDATION” as an example. The OU name “VALIDATION” and the domain “val.ctc.se.com” will be needed again in Assign user to group(s), page 227.

In ADUC (**Active Directory Users and Computers**), expand the domain *val.ctc.se.com*, right click on the OU *VALIDATION*, then click on **New/User** on the pop-up menu.

The new user is to be created with the detailed information as below:

- **First name**: Alice
- **Last name**: Wang
- **Full name**: AWang
- **User logon name**: Alice Wang
- **User logon name (pre-Windows 2000)**: Alice Wang

Note that the full name “AWang” is the username to be used for authentication at PowerLogic P5 end.

After the input of the above information, click on **Next >** button to next page.

> **NOTE:** If the user is newly created, do not check the *User must change password at next logon* option, as there is no mechanism at PowerLogic P5 to change the password. If it is required to force the user to change the initial password then they will need to log in with a PC and change the initial password before they can authenticate with PowerLogic P5.

Create the group

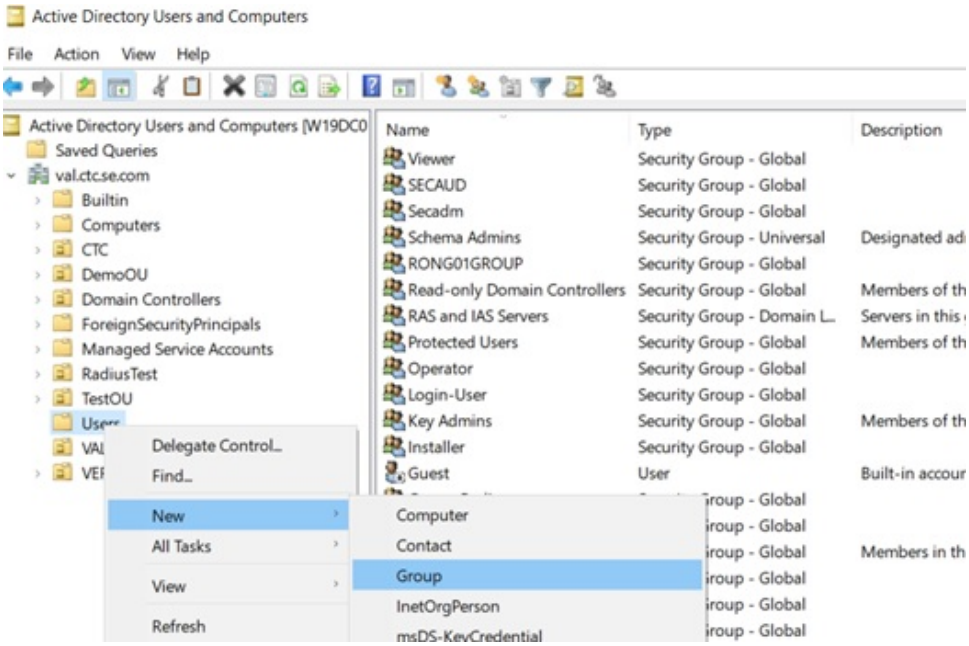
In ADUC, expand the domain *val.ctc.se.com*, right click on the Common Name (CN) *Users*, then click on **New/Group** on pop-up menu.

The new group is to be created with the detailed information as below:

- **Group name**: Relay Engineer
- **Group name (pre-Windows 2000)**: Relay Engineer
- **Group scope**: Global
- **Group type**: Security

Click **OK** button.

Figure 168 - Create the group in Users common name



Assign user to group(s)

Add the user “AWang” to the group “Relay Engineer” with the detailed information as below:

- **Select this object type**: Groups or Build-in security principals
- **From this location**: val.ctc.se.com
- **Enter the object names to select (examples)**: Relay Engineer

Click **OK** button.

If you want to assign the user to multiple groups, you can repeat the above step.

Configuration of the RADIUS server at CAP end

This step is only needed for older PowerLogic P5 versions which only have the RADIUS client. If your PowerLogic P5 version is V01.500.101 or later you can skip to the next section.

The setting at CAP end consists of two steps:

1. Mapping between AD groups and device roles
2. Setting the shared secret

Mapping between AD groups and device roles

Use the Laptop 1 to SSH into CAP with command:

ssh capuser@10.10.10.99 -p 4422

NOTE: capuser is the only username for managing CAP when the installation is completed. CAP will ask you the password for capuser.

After successful login, enter the following command to enter the CAP setting:

cap-config

When the CAP setting menu is displayed, navigate to the following item:

- **Configuration/Configure RADIUS/AD proxy/Edit user configuration file**

If you want to map the “ENGINEER” role in PowerLogic P5 to the “Relay Engineer” group in AD server, do the following:

- In the editor, for the user group “Relay Engineer” in common name “Users”, and domain “val.ctc.se.com”, add the following lines
  - DEFAULT Ldap-Group == “CN=Relay Engineer,CN=Users,DC=val,DC=ctc,DC=se,DC=com”

    Reply-Message = “ENGINEER”

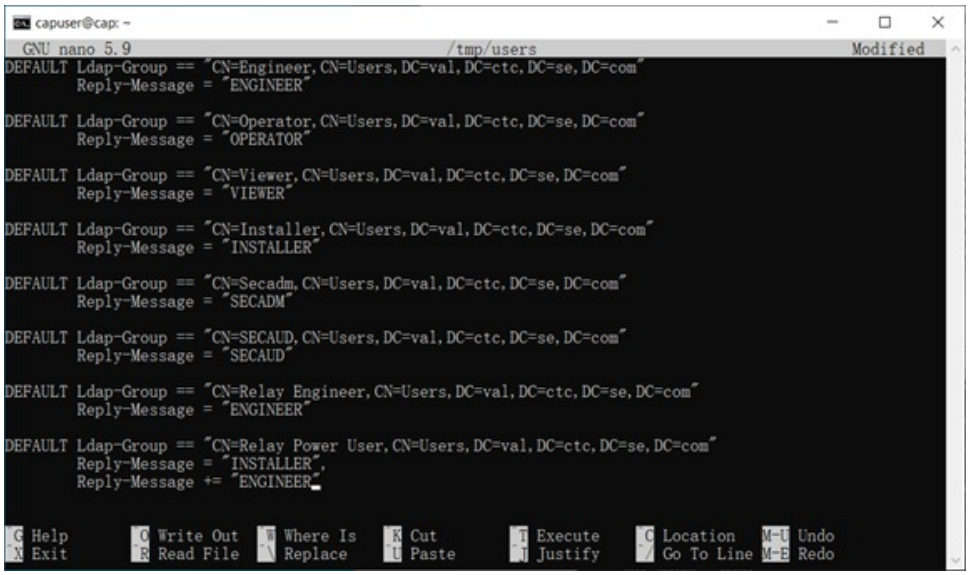
If you want to assign multiple roles in the PowerLogic P5 to one specific group in AD server, for example to map “INSTALLER” and “ENGINEER” roles to group “Relay Power User”, add the following lines:

- DEFAULT Ldap-Group == “CN=Relay Power User,CN=Users,DC=val,DC=ctc,DC=se,DC=com”

  Reply-Message = “INSTALLER”,

  Reply-Message += “ENGINEER”

Figure 169 - CAP server RADIUS configuration for mapping groups to roles



When the above modification is done, press **Ctrl + X**, then press **y** and **Enter** to confirm the modification and exit the nano editor with the changes saved.

The CAP will now restart the RADIUS service. To confirm the RADIUS service is successfully restarted, navigate to the following menu to check the logs:

- **Configuration/Configure RADIUS/AD proxy/Read logs**

The message “Ready to process requests” means that the RADIUS server has successfully restarted.

Setting the shared secret

The shared secret is a text string that serves as a password between the RADIUS client (PowerLogic P5) and the RADIUS server (CAP).

To set the shared secret, navigate to the following menu:

- **Configuration/Configure RADIUS/AD proxy/Edit clients configuration file**

Add the following lines to the file:

- client ctc-val-test {
  ipaddr = 10.10.10.0/24
  secret = Test*#12
  }

The client name can be any text as you want, as an example we have used “ctc-val-test” here.

The ipaddr shall be the network segment in which the PowerLogic P5 devices are located, with 24 being the length of the subnet mask, the specified network segment is 10.10.10.0 to 10.10.10.255 in this case.

Configuration at the PowerLogic P5 end

Open the CAE software installed on Laptop 2, go to the menu **SECURITY SETTINGS/Authentication Configuration**.

LDAP setting

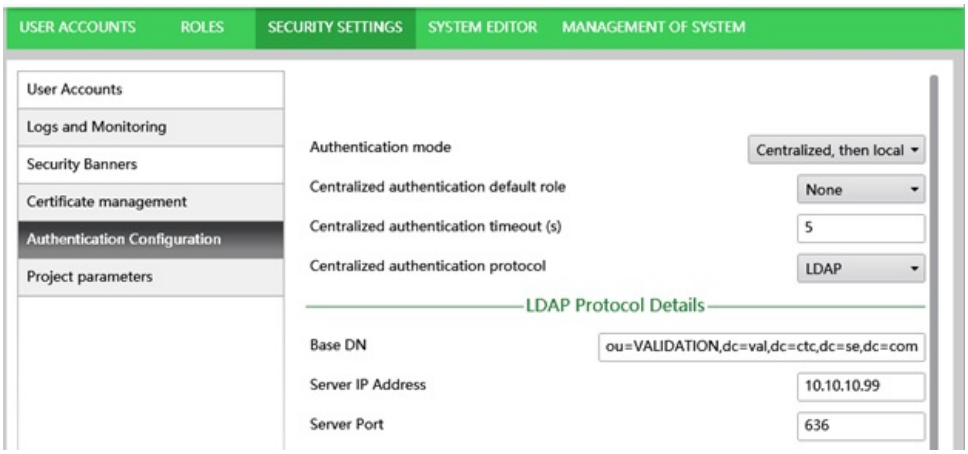
PowerLogic P5 versions later than V01.500.101 is equipped with an LDAP client thus it is recommended to use LDAP as it offers better security than RADIUS.

The LDAP protocol details for the setting are as following:

- In the section **LDAP Protocol Details**, for **Base DN**, for the OU *VALIDATION* and the domain *val.ctc.se.com* in this example, use value “ou=VALIDATION, dc=val,dc=ctc,dc=se,dc=com”.
- Value of input box **Server IP Address** and **Server Port**:
  - If you are using CAP as a proxy between PowerLogic P5 devices and the AD server, provide the proxy IP address and port number.
  - If PowerLogic P5 devices are connecting directly to the AD server, provide the AD server address and port number instead.

    NOTE: The port number depends on the type of protocol to be used. For detailed information about the port number and corresponding protocols please refer to the CAE and CAP documentation, and the setting of your AD server. PowerLogic P5 supports LDAP and LDAP + StartTLS protocols.

Figure 170 - LDAP setting in CAE



- To grant the ”ENGINEER” role privilege to the “Relay Engineer”, click **Add a new group** button, input name *Relay Engineer* in the text box above the button, and check *ENGINEER* in the list of **Role(s)**, then click **Add a new group** button again.

Figure 171 - Map one role to one group

- To grant the ”ENGINEER” and “INSTALLER” roles privilege to the “Relay Power User”, click **Add a new group** button, input name *Relay Power User* in the text box above the button, and check *ENGINEER* and *INSTALLER* roles in the list of **Role(s)**, then click **Add a new group** button again.

Figure 172 - Map multiple roles to one group

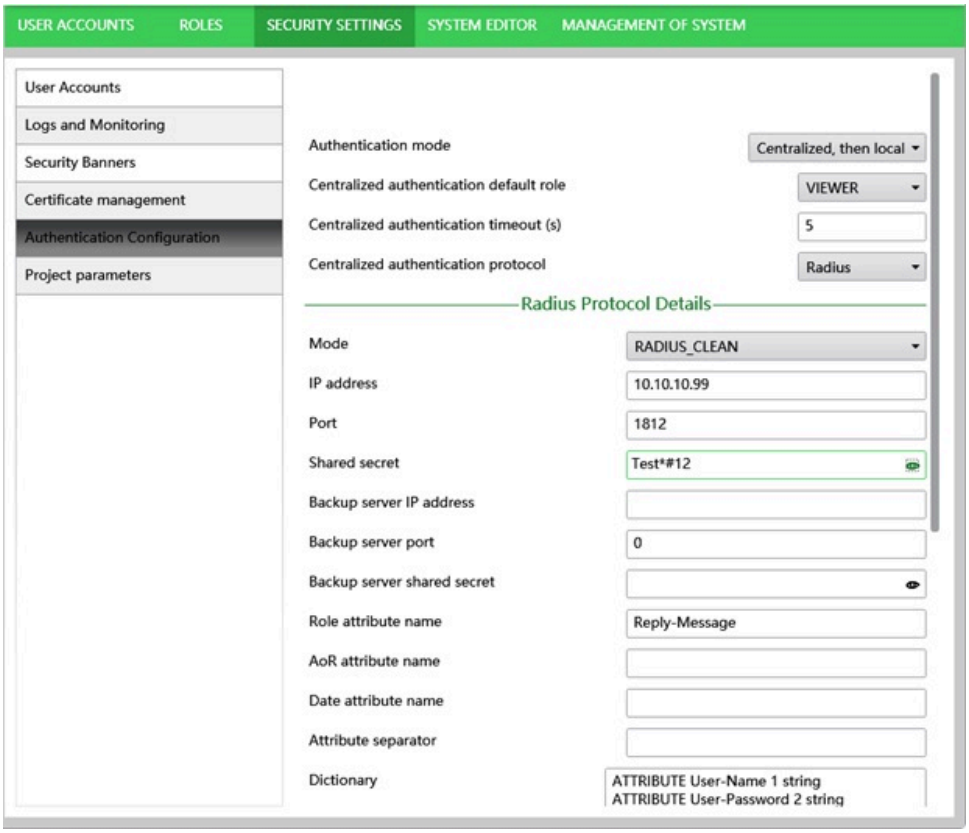
RADIUS setting

For older PowerLogic P5 versions, the only option is to connect to CAP over RADIUS.

Most of the settings can be left as defaults, except for the following in the section **LDAP Protocol Details**:

- **Shared secret**: it must be the same as set in the CAP server, which is “Test*#12” in this example.
- **Role attribute name**: it must be “Reply-Message”.
- **Mode** and **Port**: For details about the settings of Mode and Port, please refer to the CAE and CAP user documentation. PowerLogic P5 supports RADIUS_CLEAN and EAP_TTLS protocols.

Figure 173 - RADIUS setting in CAE for using CAP as proxy



Congratulations! After completing the above steps, user Alice WANG can use her credentials set by the AD server for PowerLogic P5 authentication and obtain the role privileges in device mapped to her user group in AD server accordingly.

RADIUS as existing authentication server

PowerLogic P5 can use a RADIUS server directly as the authentication server — no AD server or CAP server is required. The RADIUS server can be in the same secure zone with the PowerLogic P5 devices, as shown in RADIUS server in the same secure zone with PowerLogic P5, page 231. Or the RADIUS sever can be in another secure zone, and the firewall is set to allow the RADIUS protocol between the PowerLogic P5 devices and the RADIUS server, as shown in RADIUS server in a different secure zone with PowerLogic P5, page 232

Figure 174 - RADIUS server in the same secure zone with PowerLogic P5

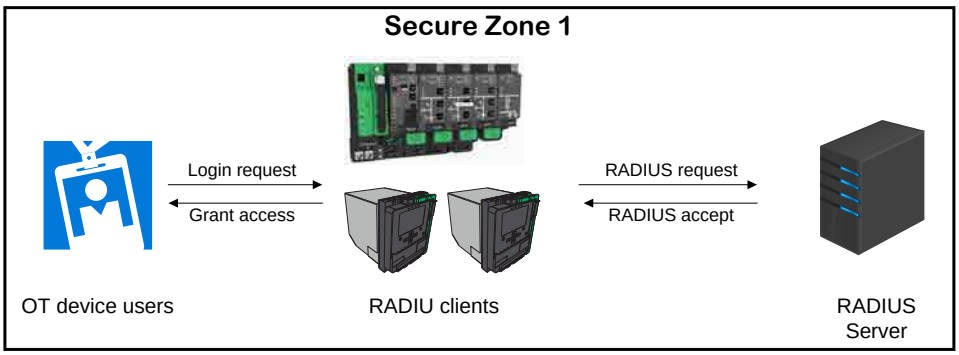
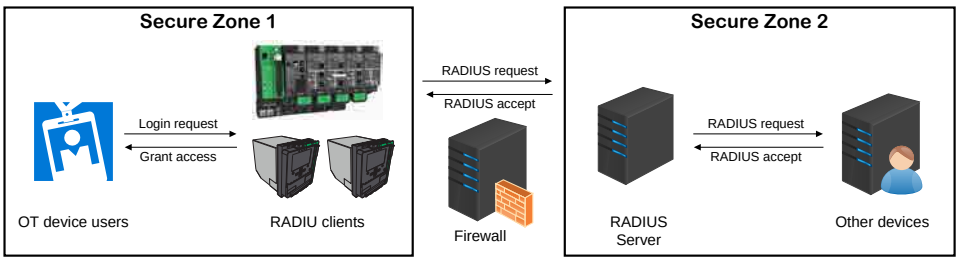


Figure 175 - RADIUS server in a different secure zone with PowerLogic P5



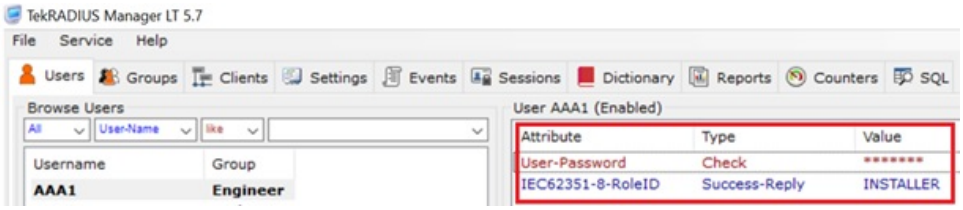
The configuration consists of 2 steps, namely:

1. Setting at the RADIUS server
2. Setting at the PowerLogic P5 end with CAE

Setting at the RADIUS sever

Using TekRADIUS as an example, the setting at the server end is as shown below.

Figure 176 - User role mapping in TekRADIUS server



On the left side you can find all the usernames and groups in the RADIUS server database. Note that the group “Engineer” here does not have any mapping relation with the roles in PowerLogic P5.

On the right side you can find the attributes for highlighted user. There are two attributes to be configured:

1. The first attribute specifies the password for user AAA1. The **Attribute** name shall be *User-Password*. The **Type** shall be *Check*. The **Value** contains the password.
2. To assign user AAA1 a role in PowerLogic P5, the 2nd attribute is needed. Its **Type** shall be *Success-Reply*. The **Attribute name** can be anything but must be the same as the Role attribute name setting in CAE. We use *IEC62351-8-RoleID* as an example. The role to be assigned to user AAA1 shall be entered in the Value field, which is *INSTALLER* in this example.

By providing the above two attributes, user AAA1 will get the INSTALLER role privilege in PowerLogic P5.

If you want to assign multiple roles to user AAA1, for example to assign “INSTALLER” and “ENGINEER” roles to AAA1, set the values of **Attribute** *IEC62351-8-RoleID* as *INSTALLER;ENGINEER* by repeating the sequence of operations above.

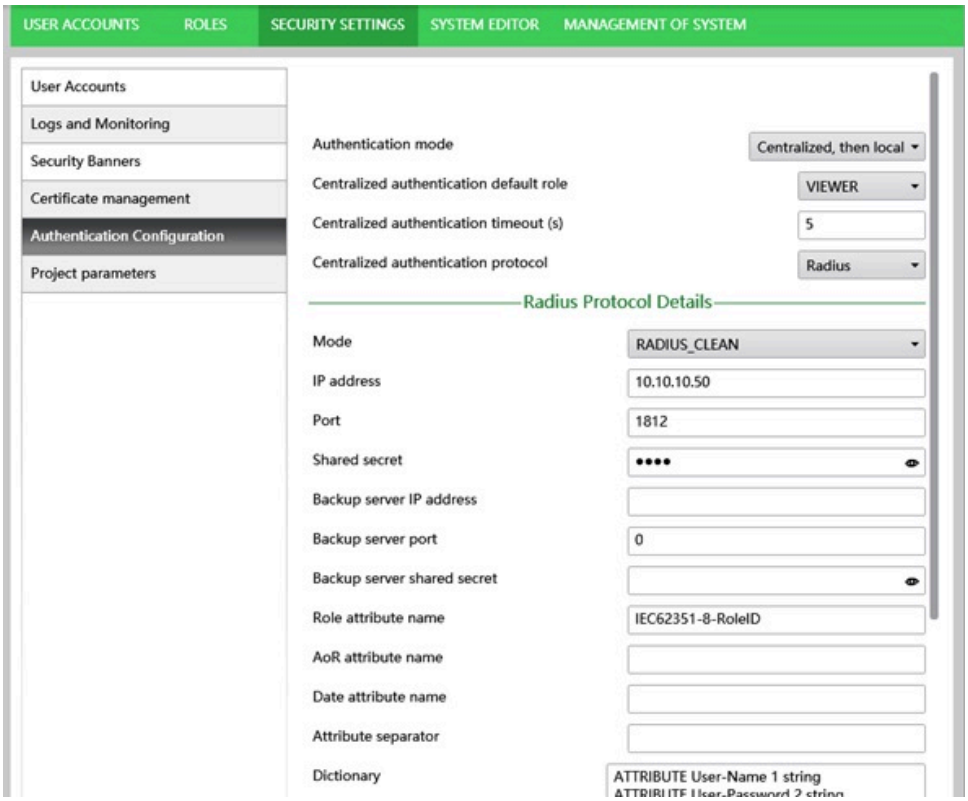
Figure 177 - Mapping multiple roles to TekRADIUS user

Setting at the PowerLogic P5 end with CAE

Open the CAE software, go to the menu **SECURITY SETTINGS/Authentication Configuration**. Choose *Radius* for **Centralized authentication protocol**. In the section of **Radius Protocol Details**, change the settings of the following items:

1. **Mode**, **IP address** and **Port number** of the TekRADIUS server: for details about the settings please refer to the CAE documentation and your RADIUS server setting. PowerLogic P5 supports RADIUS_CLEAN and EAP_TTLS
2. **Shared secret** needs to be the same as set in the TekRADIUS server.
3. **Role attribute name** must be the same as the TekRADIUS setting which is “IEC62351-8-RoleID” in this example

Figure 178 - CAE setting for RADIUS server



Now the user AAA1 can authenticate to PowerLogic P5 with the credential set in the TekRADIUS server and obtain accordingly the role privileges as specified in the TekRADIUS server.

Port hardening

It is possible to disable PowerLogic P5 communication ports from the local panel, eSetup Easergy Pro, or web HMI with ENGINEER access right.

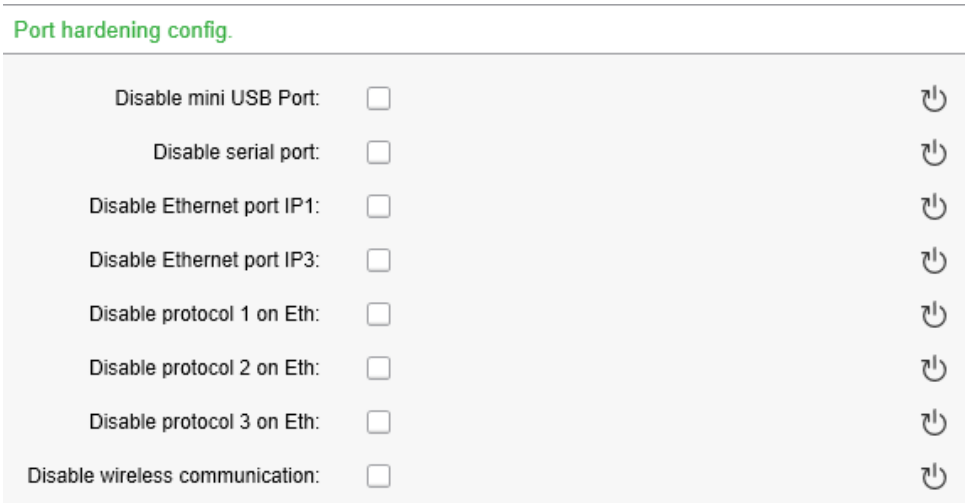
Physical ports which can be disabled:

- Front mini-USB port (for eSetup Easergy Pro connection)
- Rear serial port
- Rear Ethernet port

Wireless communication through Zigbee board can also be disabled.

The figure below shows the Port Hardening Configuration settings in eSetup Easergy Pro/**COMMUNICATION**/**Protocol Configuration**/**Port hardening config.**:

Figure 179 - Port hardening configuration settings in eSetup Easergy Pro



The port hardening can also be set from the local panel through the **Port hardening** configuration view of the **General** menu.

When the ports or the protocols on the Ethernet module are disabled or enabled, reboot of the PowerLogic P5 protection relay is needed.

> **NOTE:** In addition to port hardening configuration, and in order to help prevent access to the communication ports on the local panel, it is possible to replace put with install physical seal (See Lock the shutter and handle, page 55).

It is possible to disable SSH protocol for the rear Ethernet ports. The setting can be made only from local panel by **General setting** / **Port hardening** / **Dis. Eth SSH**.

Security event logging

The function of security event log and back up remotely the logs to Syslog server is only available in Advanced CS level. The security logs are generated by PowerLogic P5 and saved locally with secured storage on FLASH memory. They are read-only and undeletable for any role. In the meantime the logs will be pushed to the Syslog server defined by CAE. Syslog server manages the logs according to customer security policy.

PowerLogic P5 does not enable by default any of logging standards listed in the table below . The logging standards can be selected in CAE according to requested logs.

Table 46 - Security logs list

Log ID	Description	BDEW	IEEE 1686–2013
CONNECTION_SUCCESS	Successful connection	■	■
CONNECTION_FAILURE	Unsuccessful connection (wrong credentials)	■	■
CONNECTION_FAILURE_AND_BLOCK	Unsuccessful connection (wrong credentials) triggering the blocking of the account	■	■
CONNECTION_FAILURE_ALREADY_BLOCKED	Unsuccessful authentication because the account is already blocked	■	■
DISCONNECTION	Disconnection triggered by user	■	■
DISCONNECTION_TIMEOUT	Disconnection triggered by timeout	■	■
FIRMWARE_UPDATE	Firmware update to IED	■	■
RBAC_UPDATE	Update of the RBAC setting in the IED		■
SEC_LOGS_RETRIEVAL	CAE extraction of security logs from IED		■
TIME_CHANGE	Time change from Easergy Pro, local HMI, Web HMI, protocol time synchronization		■
PORT_MANAGEMENT	Port hardening operations		■
SECURITY_UPDATE	Update of the Security policy database		■

Upgrades management

When the PowerLogic P5 protection relay firmware is upgraded – security configuration remains the same until changed, including usernames and passwords. It is recommended security configuration is reviewed after an upgrade to analyze rights for new or changed device features and revoke or apply them according to your company’s policies and standards.

Security functionality verification

When the Cybersecurity functionalities have been configured, it is recommended to verify that the following functions are working as intended:

- RBAC function is making sure that user cannot perform actions for which he does not have privilege.
- Security event logs (CS Advanced only) are properly generated in PowerLogic P5 locally and the remote Syslog server (if configured) keeps record of them.
- Disabled logical and physical ports can no longer be accessed.

It is recommended to repeat the above tests after firmware update or security policy update.

Use

Introduction

The local panel can be used for both entering all the data required for operation of the PowerLogic P5 protection relay and accessing the data for equipment management.

The following tasks can be handled from the local panel:

- Controlling switchgear units:
  - View equipment status on an animated mimic diagram
  - Local opening and closing of up to 6 devices controlled by PowerLogic P5
- Read out the list of enabled protections
- Readout and modification of settings
- Readout of live operating data including waveforms
- Read out logic status signals
- Readout of operating data logs and of monitoring signal logs
- Readout of event logs after overload situations, ground faults, or short circuits in the power system
- Read out the PowerLogic P5 protection relay's module versions
- Device resetting and triggering of additional control functions used in testing and commissioning
- Test the protection relay with dedicated IED modes (contact outputs forced or not)
- Entering a password according to different access rights for settings and operations (see Cybersecurity, page 191)

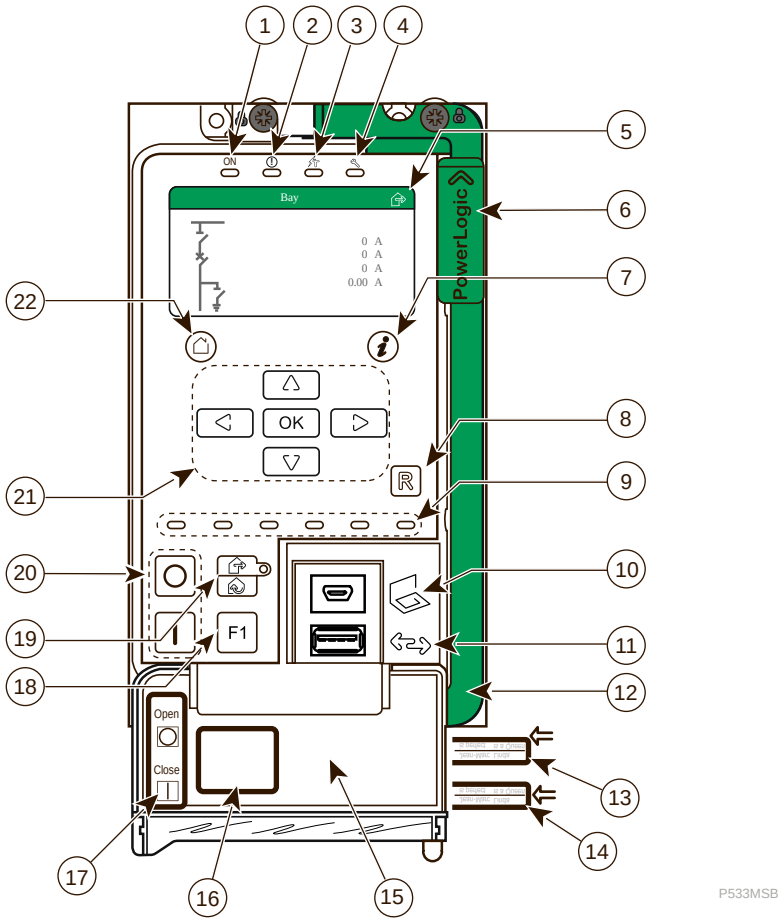
Control is also possible through the PC interface. This requires a suitable PC installed with a specific operating program called eSetup Easergy Pro (see eSetup Easergy Pro, page 257).

Local panel

Presentation

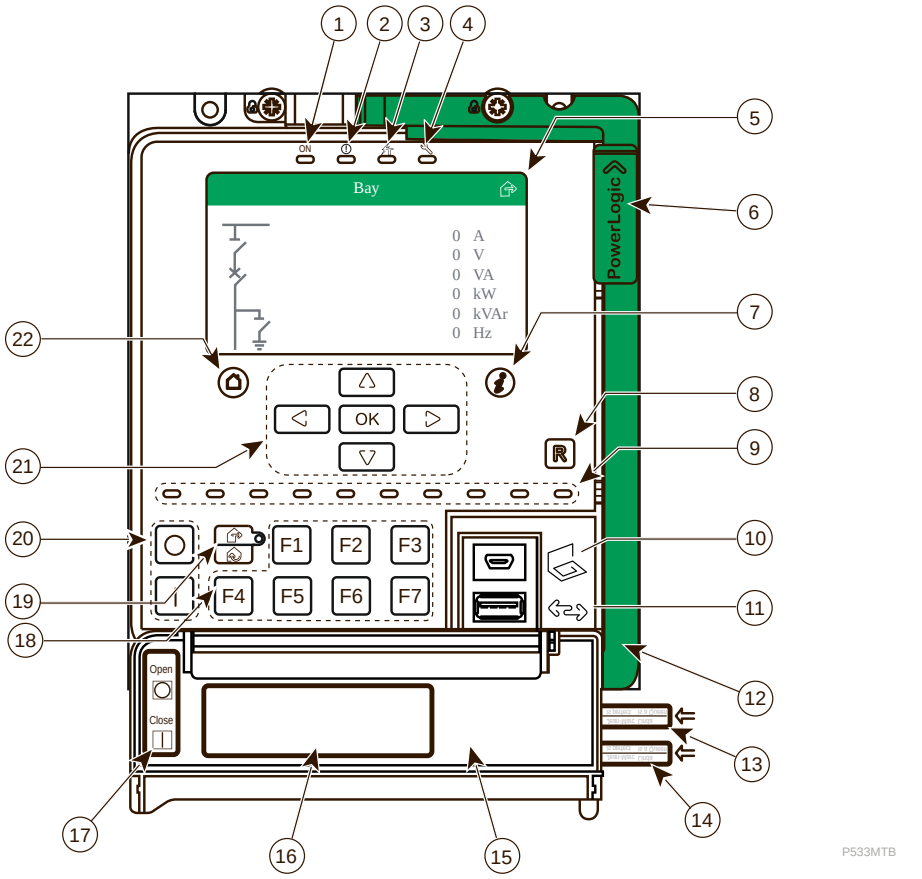
The PowerLogic P5 protection relay is equipped with a user friendly local panel.

Figure 180 - Local panel of PowerLogic P5x20



①	Power ON/OFF LED	⑫	Handle
②	Alarm LED	⑬	Label for protection relay name (inserted in the shutter)
③	Trip LED	⑭	LED identification label (inserted in the shutter)
④	Maintenance/Test LED	⑮	Shutter
⑤	Graphic 192 x 96 monochrome LCD screen	⑯	Label for programmable function key (stuck on the back of the shutter)
⑥	Handle lock (movable up and down)	⑰	Label for CB (Circuit Breaker) open and CB close keys (stuck on the back of the shutter)
⑦	Information key	⑱	F1 function key
⑧	Reset key	⑲	Remote Control/Local Control key
⑨	6 LEDs, user programmable	⑳	CB (Circuit Breaker) Open (upper) and CB Close (lower) keys
⑩	Mini-USB connector for connecting laptop (behind a plastic cover)	㉑	Navigation keypad and confirmation key
⑪	USB connector for data transfer (behind a plastic cover)	㉒	Home key

Figure 181 - Local panel of PowerLogic P5x30



①	Power ON/OFF LED	⑫	Handle
②	Alarm LED	⑬	Label for protection relay name (inserted in the shutter)
③	Trip LED	⑭	LED identification label (inserted in the shutter)
④	Maintenance/Test LED	⑮	Shutter
⑤	Graphic 480 x 272 color LCD screen	⑯	Label for programmable function key (stuck on the back of the shutter)
⑥	Handle lock (movable up and down)	⑰	Label for CB (Circuit Breaker) open and CB close keys (stuck on the back of the shutter)
⑦	Information key	⑱	F1 - F7 function keys
⑧	Reset key	⑲	Remote Control/Local Control key
⑨	10 LEDs, user programmable	⑳	CB (Circuit Breaker) Open (upper) and CB Close (lower) keys
⑩	Mini-USB connector for connecting laptop (behind a plastic cover)	㉑	Navigation keypad and confirmation key
⑪	USB connector for data transfer (behind a plastic cover)	㉒	Home key

Push buttons

Symbol	Function
	HOME/Cancel push-button for returning to the previous view. To return to the default screen of the LCD display, keep the button pressed for 3 seconds.
	INFO push-button for viewing additional information.
	Reset key to release latches and reset LED status.
	1 programmable function push-button for PowerLogic P5x20 (see Object control with function keys, page 539)
 to 	7 programmable function push-buttons for PowerLogic P5x30 (see Object control with function keys, page 539)
	ENTER push-button for activating or confirming a function.
	UP navigation push-button for moving up in the menu or increasing a numerical value.
	DOWN navigation push-button for moving down in the menu or decreasing a numerical value.
	LEFT navigation push-button for moving back across a menu or selecting a digit in a numerical value.
	RIGHT navigation push-button for moving forwards across a menu or selecting a digit in a numerical value.
	Circuit breaker ON push-button (see Object control with I and O buttons, page 540)
	Circuit breaker OFF push-button (see Object control with I and O buttons, page 540)
	This push button allows the user to set the PowerLogic P5 protection relay to remote control mode or local control mode.

NOTE: The programmable function push buttons, the Local/Remote control key and the control circuit breaker push buttons are protected by a shutter in normal operation. This shutter can be sealed (see Lock the shutter and handle, page 55).

LED indicators

Status indicators

This includes the 4 LEDs located on top of the LCD representing the different status of the PowerLogic P5 protection relay regarding power, alarm, trip, and operation mode (refer to item 1 to 4 in Local panel of PowerLogic P5x20, page 237 and Local panel of PowerLogic P5x30, page 238) and the LED associated with the "Local/Remote" push button (refer to item 19 in Local panel of PowerLogic P5x20, page 237 and Local panel of PowerLogic P5x30, page 238).

Table 47 - The states of the status indicators

Indicators	States		
	OFF	ON	Flash
ON	Power OFF	Power ON	-
	No alarm	-	Alarm
	No trip	Trip	-
	In service	Maintenance	Test/Test-block mode
	In local control mode	In remote control mode (steady green)	-

Configurable LEDs

These LEDs can be configured in three different colors: green, red and yellow, and be individually latched or unlatched (see LED matrix, page 531).

These LEDs are configured by default according to LED1 to LED6 on PowerLogic P5 x20, page 240 and LED1 to LED10 on PowerLogic P5 x30, page 240.

Table 48 - LED1 to LED6 on PowerLogic P5 x20

Color	LED 1	LED 2	LED 3	LED 4	LED 5	LED 6
PowerLogic P5U20						
Green	CB Open					
Yellow		Trip Circuit Supervision (TCS) Alarm			Therm Alarm	
Red	CB Closed		I Trip	IN Trip		
PowerLogic P5V20						
Green	CB Open					
Yellow		TCS Alarm				
Red	CB Closed		V Trip	VN Trip	f Trip	

Table 49 - LED1 to LED10 on PowerLogic P5 x30

Color	LED 1	LED 2	LED 3	LED 4	LED 5	LED 6	LED 7	LED 8	LED 9	LED 10
Green	CB Open									
Yellow		TCS Alarm			Therm Alarm					
Red	CB Closed		I Trip	IN Trip			V Trip	VN Trip	f Trip	

Customising the local panel

The local panel of the PowerLogic P5 protection relay can be customised with four labels for:

- Configurable LEDs
- Configurable function keys

- Circuit breaker control push buttons
- Name of the protection relay or feeder

  NOTE: The PowerLogic P5 protection relay is delivered with:

  - A label of configurable LEDs with default configuration (English version; see LED1 to LED6 on PowerLogic P5 x20, page 240 and LED1 to LED10 on PowerLogic P5 x30, page 240)
  - A label in color for the circuit breaker control push buttons

The different labels can be defined with eSetup Easergy Pro in **DOCUMENTATION/Documentation view**.

The labels can be exported from the **Documentation view** to a pdf file by clicking the **Export PDF** button at bottom right, which then can be printed.

When the labels are printed and adjusted:

- Insert the label for the configurable LEDs in the shutter (see 14 in Local panel of PowerLogic P5x20, page 237 and Local panel of PowerLogic P5x30, page 238)
- Stick the label for the programmable function push buttons on the back side of the shutter (see 16 in Local panel of PowerLogic P5x20, page 237 and Local panel of PowerLogic P5x30, page 238)
- Stick the label for the circuit breaker control push buttons on the back side of the shutter (see 17 in Local panel of PowerLogic P5x20, page 237 and Local panel of PowerLogic P5x30, page 238)
- Insert the label for the protection relay name in the shutter (see 13 in Local panel of PowerLogic P5x20, page 237 and Local panel of PowerLogic P5x30, page 238)

Introduction to the LCD display

PowerLogic P5 protection relay service cycle

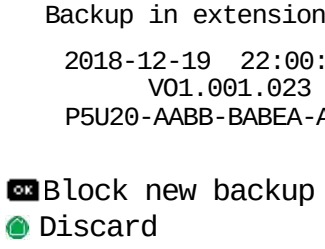
During the start-up of the PowerLogic P5 protection relay, a series of boot messages are displayed to guide the user through the whole process.

The start up process may be different dependent on whether the optional extension module is installed.

If there is no extension module installed, the protection relay enters into the operation mode and displays the default screen (e.g. the Mimic screen), which can be set through eSetup Easergy Pro in the **GENERAL** menu.

If the extension module is installed, the PowerLogic P5 protection relay checks whether the content of the extension module is a backup of its existing configuration and settings by comparing the version numbers.

Figure 182 - Message on handling the existing content in the extension module



If it is, the PowerLogic P5 protection relay proceeds to the default screen; If it isn't, a message is displayed, prompting the user to either keep or discard the content

of the extension module. If the user selects the “Block new backup” option, the content is kept, the PowerLogic P5 protection relay will block the backup operation; If the user selects the “Discard” option, the protection relay directly reconfigures from the extension module.

When the PowerLogic P5 protection relay is in operation mode, it is possible to switch to the main menu screen by pressing key. Depending on the user role, the user can also change the device settings at any time.

If an event or alarm occurs during operation, a popup message is permanently displayed on the LCD screen until it is acknowledged using the key.

If a fault occurs during operation, a popup alarm message is permanently displayed on the LCD screen, press key to access the **Fault recorder** screen.

If there is an alarm message displayed and no action on the keypad for 5 minutes, the PowerLogic P5 protection relay will jump to the default screen and then display the alarm message again automatically.

If there is no alarm message displayed, the default screen is displayed automatically.

Menu structure

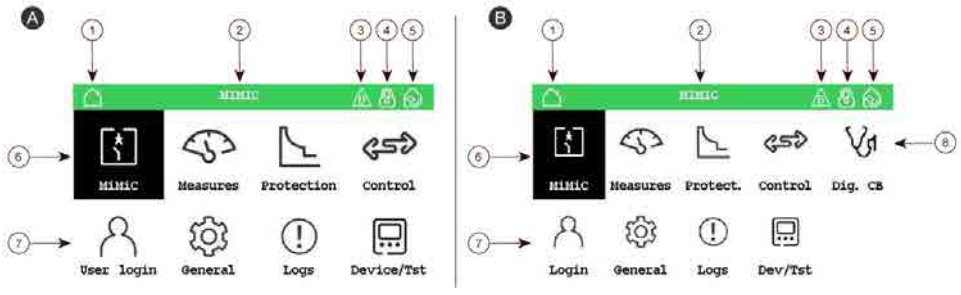
The PowerLogic P5 protection relay has two levels of menus: the main menu (home menu) and sub-menus.

> **NOTE:** The hierarchy and navigation of the menu structure are the same on PowerLogic P5x20 and PowerLogic P5x30, but due to a larger resolution, the PowerLogic P5x30 LCD color screens can display data and graphics in greater detail.

The PowerLogic P5 device is delivered with auto-login feature. It will be disabled when the passwords for all three levels are changed from the default ones. For the default passwords for all the levels, refer to Default settings, page 213.

Main menu (home menu)

Figure 183 - The main menu with menu item Mimic in focus



A	Main menu (Digital CB protocol is not configured)	B	Main menu (Digital CB protocol is configured)
1	Home menu icon	5	Remote/Local control icon
2	Full name of the menu item in focus	6	Menu item in focus
3	Cybersecurity level icon	7	Menu item not in focus
4	Padlock icon	8	Digital Circuit Breaker monitoring icon

The main menu screen has 2 widgets: the top title bar, and the main display area. The top title bar shows the following items:

- Menu name: full name of the menu item that is being selected (the names next to the menu icons use their short forms)
- Home icon: located on the left side of the top title bar, indicates that the current screen is the home screen of the LCD display
- Cybersecurity level icon: located on the right side of the top title bar. stands for the Basic Cybersecurity level, stands for the Advanced Cybersecurity level.
- Padlock icon ( ): located on the right side of the top title bar, indicating that no user has logged in to the device; the icon disappears when any user has logged in.
- Remote/Local control icon: located on the right end of the top title bar, indicates the protection relay's current control mode

Figure 184 - The remote/local control icons

Remote mode

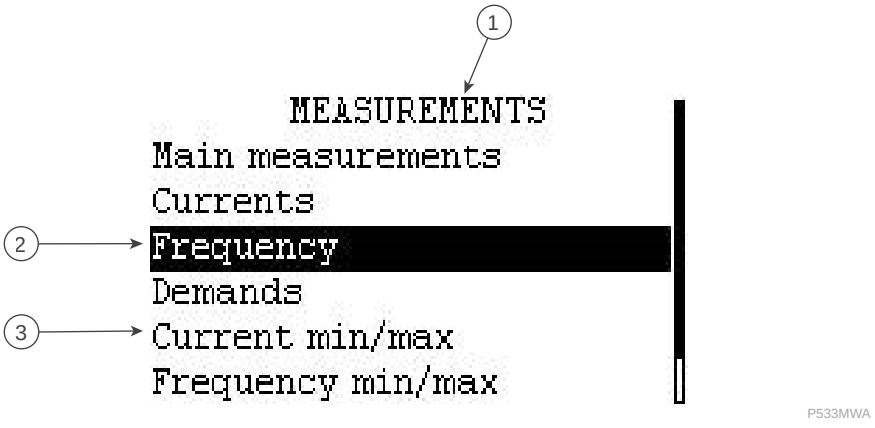
Local mode

The main display area lists all the menu items (sub-menus) of the PowerLogic P5 protection relay.

In the main menu, pressing the navigation keys on the local panel moves the focus onto a main menu item (sub-menu). The sub-menu title is displayed in the top title bar of the main menu screen. Pressing OK allows the user to enter the highlighted sub-menu.

Sub menus

Figure 185 - The Measurement sub-menu



1	Title of sub-menu	3	Menu item not in focus
2	Menu item in focus		

In the sub-menu, pressing ▲ or ▼ key moves the focus onto a sub-menu item and pressing OK selects the item and allows the user to enter the setting page of the item.

NOTE: There could be more menu items than is able to be displayed in the view. The user needs to scroll to these items using the ▼ key.

Data/setting page

Some sub-menu items may have more than one data/setting pages, which is indicated by an arrow on either the left or right end, or by arrows on both ends of the title bar:

- Arrow on the right end
  Press the ▷ key scrolls the screen to the next data/setting page.
- Arrow on the left end
  Press the ◁ key scrolls the screen to the previous data/setting page.
- Arrows on both the left and right ends
  Press the ◁ or ▷ key scrolls the screen to the previous or next data/setting page, respectively.

Upon seeing the desired data/setting page, press OK to allow the user to enter the data/setting page, then press the △ or ▽ key moves the focus onto each parameter field.

NOTE: There may be more parameters than the view can display. The user needs to scroll to these parameters using the ▽ key.

When an editable parameter is in focus, press OK to open the parameter setting view and enable the user to change the value or option by pressing the navigation arrow keys. When a non-editable parameter is in focus, press OK key to pop up a message indicating that the parameter is not editable. When the user is not fully authorised to edit the setting, press OK key to pop up a "Permission denied" message.

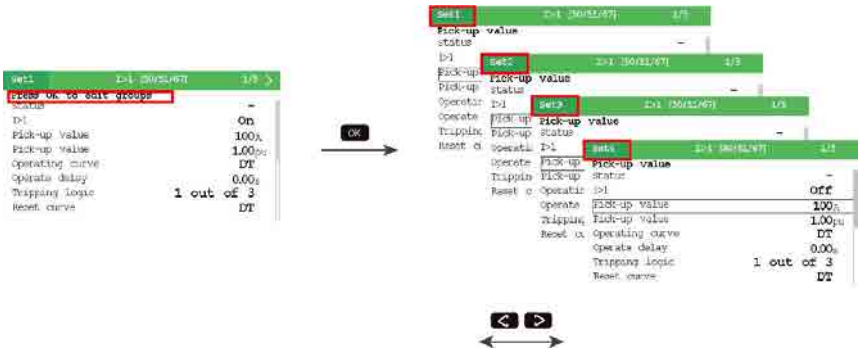
When changing the settings, use the navigation keys according to the following instructions to get the result quickly:

- For selecting options, use the △ and ▽ keys;
- For changing the value of integer numbers, use either the △ and ▽ keys, or the ◁ and ▷ keys;
- For changing the value of float numbers, first use the △ and ▽ keys to quickly approach the integer part of the number in steps of 1 and then use the ◁ and ▷ keys to adjust the decimal part in steps of 0.01.

In the protection menu, some protection stage items have a first setting page with more than one view. These views belong to different setting groups of the protection stage. In this case, upon selecting the menu item, an additional text line "Press OK to edit groups" is displayed at the top of the main display area to indicate that here the user can edit the settings of different setting groups.

Press the OK key to enter the group editing status. Press the ◁ and ▷ keys to scroll to the setting view for the desired setting group.

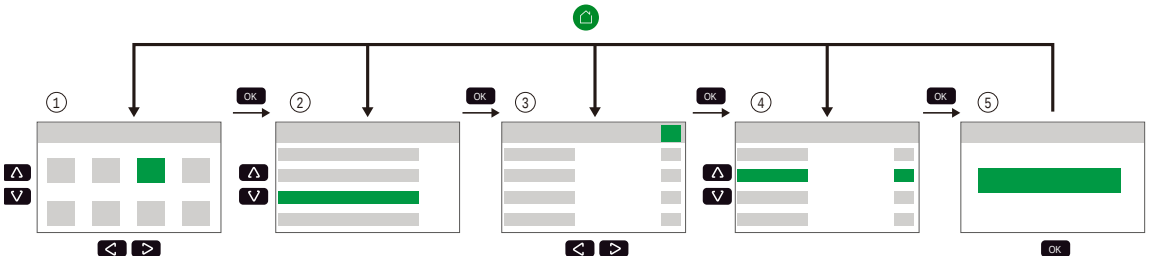
Figure 186 - Example of a data/setting page with 4 setting views



Moving in the menu structure

The following image describes the operation to navigate in the menu structure.

Figure 187 - Moving in the menu structure of the PowerLogic P5 protection relay



1	Main menu	4	Data/setting page (parameter selecting view)
2	Sub-menu	5	Parameter editing view
3	Data/setting page (page selecting view)		object in focus

Press ◁, ▷, △ and ▽ keys to move focus in menu.

Press OK key to enter the sub menu (2), the data/setting page selecting view (3), the parameter selecting view (4), or the parameter editing view (5), depending on where the user is situated in menu structure.

OK key is also used to confirm and finalise the editing in the parameter editing view.

Press ⌂ key once to return to previous view.

Keep pressing the ⌂ key for 3 seconds to display default screens.

Moving default screens and mimics

There are two ways to display default screens:

- keep pressing the ⌂ key for 3 seconds
- make no action on the keypad for 5 minutes.

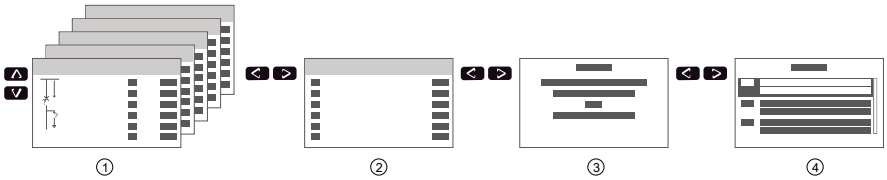
It is possible to scroll between visible mimics (per setting) and between default screens.

To scroll between mimics and other default screens, please press ◁ and ▷ keys to scroll between mimics and **Alarm list**.

In mimics of default screen, use △ and ▽ keys to scroll between **Mimic 1** and **Mimic 10**.

> **NOTE:** If **Mimic 2** to **Mimic 10** are set to invisible, press △ and ▽ keys will not scroll to other mimics from **Mimic 1**.

Regardless of which mimic is actually displayed, pressing ▷ key will scroll to **Main measurements** window. When pressing ◁ key in **Main measurements** window, **Mimic 1** will be displayed.



P533S4A

1	Mimics	2	Main measurements
3	Firmware version	4	Alarm list

Login and logout

NOTE: For more details about password management, see relevant sections in Cybersecurity, page 191.

Login

The user may need to log in before changing settings or accessing the data protected by password. The PowerLogic P5 device is delivered with auto-login feature. It will be disabled when the passwords for all three levels are changed from the default ones. For the default passwords for all three levels, refer to Default settings, page 213.

Except from the home screen or alarm popup screen, access the User Login screen by pressing the *i* key on the local panel and press the OK key. This feature allows you to access the User Login screen from anywhere in the menu structure instead of returning to the Home page.

The following login procedure starts from the main menu.

1. Press the navigation keys and the OK key to enter the User Login menu from the main menu screen.

   The screen displays the Login view with the focus on the "Name" field.
2. Press OK to show the user list, which displays the three default user levels provided by the PowerLogic P5: Engineer Level, Operator Level and Installer Level.
3. Press △ or ▽ key to select a user name from the user list and then press the OK key to confirm your choice.
4. Enter the password by first pressing ◁ or ▷ key to select the code position, and then press △ or ▽ key to select different letter or digits and press the OK key to confirm.

   NOTE: After a correct password is entered, the LCD display returns to the home screen and the padlock icon disappears from the screen title bar, indicating that the user is now able to view/edit the settings, depending on the access right level of the user type.

Logout

By default, the user is automatically logged out if there is no action on the keypad for 3 minutes.
The user can also logout manually by first going to the User Login screen from the local panel and then pressing the OK key.

NOTE: Except from the home screen or alarm popup screen, access the User Login screen by pressing the *i* key on the local panel and press the OK key. This feature allows you to access the User Login screen from anywhere in the menu structure instead of returning to the Home page.

Adjusting the LCD contrast (for PowerLogic P5x20)

The LCD contrast of the PowerLogic P5x20 protection relay can be adjusted according to the following steps:

1. On the local panel, select the **Device/Test** menu icon and then press the OK key to enter sub-menu.
2. Press ▽ key to select **Contrast of LCD**.
3. Press OK key twice to enter the setting page of LCD contrast.

4. The setting range of contrast is 1 to 15. To increase contrast, press ▲ or ▶, to decrease, press ▼ or ◀. After setting, press OK key to confirm. The contrast of LCD will be changed after confirmed.
5. Press ⌂ key to go back previous view, or keep press the key for 3 seconds to go back to default screen.

   NOTE: The LCD contrast can alternatively be adjusted by pressing the key and then pressing the ▲ and ▼ key. The contrast changes incrementally with every step but the screen does not display the values.

Changing language

The interface language can be changed on the local panel according to the following steps:

1. Press the navigation keys to select the **General settings** menu from the main menu screen, then press OK key to enter. The screen displays the **General settings** menu with the focus on the "Language" option.
2. Press the OK key to enter the Language setting page.
3. Press the OK key to focus on the setting item.
4. Press the OK key again to bring up the language list.
5. Press the ▲ or ▼ key to select the desired language and then press the OK key to confirm the selection.

   NOTE: The interface language can alternatively be changed through eSetup Easergy Pro in the **GENERAL** menu/**System info** sub-menu.

Changing the parameters

⚠WARNING

UNINTENDED EQUIPMENT OPERATION

Make sure that the reboot of the protection relay has no impact on people and equipment.

Failure to follow these instructions can result in death, serious injury, or equipment damage.

After changing some settings, the protection relay needs to reboot. During this time, the device is not operational.

Parameters can be changed on the setting pages of certain sub-menus:

1. In the main menu, enter the menu item that relates to the function you need to access.
   Refer to Main menu (home menu), page 242 for how to access the menu items.
2. In the sub-menu, select the sub-menu item that includes the parameter you want to change.
   Refer to Sub menus, page 243 for how to access the sub-menu items.
3. With the related sub-menu item selected, press ◀ or ▶ key to scroll to the specific setting page on which you can find the parameter and then press OK to enter the setting page.
4. Press the ▲ or ▼ key to move the focus onto the parameter field and then press the OK key to start editing the parameter.

5. Use the navigation keys to change the value of the parameter and then press the OK key to confirm your change.
   Refer to Data/setting page, page 245 for how to use the navigation keys tactically.
6. Press the key once to go back to the previous view in the menu, or press it for 3 seconds to return to the default screen.

Manage the alarm messages

Handling the pop-up alarm message

When an alarm message box pops up on the LCD screen, the user can acknowledge the message and close the message box by pressing the R key. Alternatively, if there is more than one alarm, the user can press the key R for about 2 seconds to bring up a dialog box where the user can opt to delete all the alarm messages.

Changing the alarm settings and viewing the alarm list

Alarm settings and list can be accessed from the Logs function group in the main menu.

The following procedure describes how to change the alarm settings and view the alarm list:

1. From the main menu, use navigation keys to select **Logs** function group, click OK key to enter sub-menu. Refer to Main menu (home menu), page 242 for how to access the menu items.
2. In the **Logs** sub-menu, select the option **Alarm logs** to enter the **Alarms** setting page.

   Refer to Sub menus, page 243 for how to access the sub-menu items.
3. Press OK key to enable selection in setting page, use △ or ▽ key to move the focus onto the parameter field and then press OK to edit setting of parameters.

   The setting page includes the following parameters:

   - **Counter**: number of alarms (from 0 to 200)
   - **Order**: scroll order (New - Old)
   - **Fault value**: fault value scaling (Primary or PU)
   - **Alarm screen**: enable alarm pop-up messages (On or Off)
   - **Event synchro.**: displaying event time not in sync (On or Off)
   - **Clear alarms**: edit DI to clear all alarms
4. Press △ or ▽ key to change the settings of the parameters and then press OK to confirm change.
5. Press the ⌂ key once to go back to the previous view in the menu, or press it for about 3 seconds to return the default screen.

   NOTE: For viewing the alarm list, press ▷ key once to go to the **Alarm list** page after Step 2.

Matrix operations

The matrix mapping operation can be performed on the local panel of the PowerLogic P5 protection relay, in the eSetup Easergy Pro software tool, or through the web HMI.

The following procedure describes the mapping operation on the local panel of the PowerLogic P5 protection relay. The operation is much easier in eSetup Easergy Pro and the web HMI due to their intuitive interfaces.

1. Select the Control function from the main menu, press OK to enter the sub-menu.
2. Press △ or ▽ key to scroll to the menu item (e.g. DI) that needs matrix mapping operation.
3. Press ◁ or ▷ key to scroll to the matrix mapping page and start the mapping operation.

   NOTE: The local panel LCD screen only shows the first line of mapping relations already existing in the configuration. If no mapping relation is available for the first line of the matrix, the screen only shows the digital input or internal signal on the left side of the screen.
4. Press △ or ▽ key to scroll to the digital input or internal signal type and then press OK to confirm. The first crossing point on the matrix line starts to blink.
5. Press ◁ or ▷ key to scroll to the crossing point for which you want to set the mapping status.

   NOTE: Some crossing points may not be visible in the screen but the user can view all the crossing points by pressing ▷ key.
6. Press ◁ or ▷ key to select the mapping status (enabled or disabled; connected or unconnected; latched or unlatched, depending on which matrix mapping operation is being performed) and then press OK to confirm.

   The screen shows the current line of mapping relations, leaving the empty crossing points invisible on the screen.
7. Press ◁ key to leave the matrix setting page and then ⌂ key to return to the preview level in the menu structure.

Controlling objects

The local panel provides buttons for directly controlling objects like circuit breaker and earth/ground switch. The user do not need to go through the menu to find out the options for closing/opening the objects.

Controlling an object with Selective Control enabled

To enable the Selective control feature, navigate to the **Control** menu/**Control objects** sub-menu of the local HMI, or to the **GENERAL** menu/**Local panel conf** sub-menu of the eSetup Easergy Pro.

When Selective Control is enabled, the control operation will include a confirmation step (select before operate).

1. Press O on the local panel to open a circuit breaker or stop a motor, or press I on the local panel to close a circuit breaker or start a motor.
2. Press the same key (O or I) again to confirm your operation, or press ⌂ on the local panel to cancel the previous operation.

Controlling an object with Direct Control enabled

To enable the Direct control feature, navigate to the **Control** menu/**Control objects** sub-menu of the local HMI, or to the **GENERAL** menu/**Local panel conf** sub-menu of the eSetup Easergy Pro (refer to Controlling an object with Selective Control enabled, page 253 and Local panel configuration, page 536 respectively).

When Direct Control is enabled, the control operation is done without confirmation.

1. Press O on the local panel to open a circuit breaker or stop a motor, or press I on the local panel to close a circuit breaker or start a motor.
2. The object in control acts according to your control operation.

Specific language file change

The PowerLogic P5 protection relay can be ordered in English version only or in English with another local language (see Order information, page 652).

The selection of the language can be done with eSetup Easergy Pro or directly on the local panel of the PowerLogic P5 protection relay (see Changing language, page 249).

Other languages can be uploaded to the PowerLogic P5 protection relay through eSetup Easergy Pro, using the Update language option from the (Tools) drop down list in the tool bar.

NOTE: The language files use the .bin extension.

For detailed list of languages, contact Schneider Electric.

Transferring data to USB memory stick

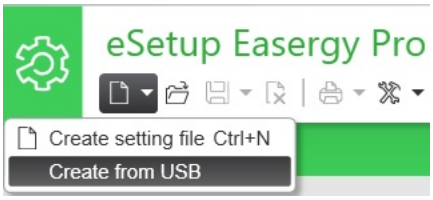
The PowerLogic P5 protection relay supports data transfer to a USB memory stick plugged into the USB 3.0 type A port located under the flap of the local panel.

Files of the following formats in the protection relay can be transferred:

File format	Description
manifest.mnfs	IED information and integrated check data
/DR/*.dat, *.cfg	Disturbance records
events.csv	IED sequence of events (maximum 2000 events)
Setting.xml	IED setting file in XML format

The settings stored in Setting.xml can be opened by eSetup Easergy Pro: click on the black triangle at right of the file button of the tool bar, select **Create from USB** to open the Setting.xml.

Figure 188 - Open Setting.xml by eSetup Easergy Pro



The features of the USB data transfer function are as follows:

- Hot-plugging is supported and the USB key status is automatically detected by the device.
- Files are copied to a sub-folder of the folder “P5bak” of the USB disk. The name of the sub-folder is composed of 3 parts: the date and time, the serial number S/N, and the model number.

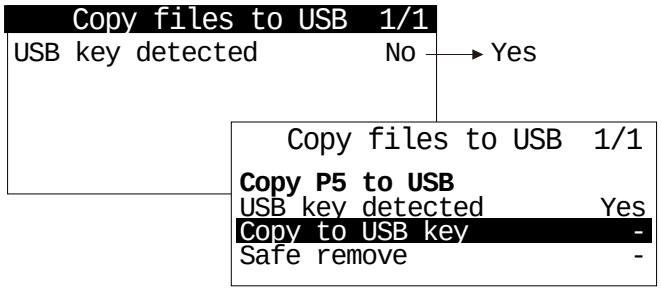
  The sub-folder is created automatically before transferring the data.
- Each file transferred is accompanied by a CRC32 check to help ensure the integrity.
- Software and hardware information is stored in the manifest file.
- Data transfer process takes about 2 to 10 minutes.
- The USB key used must be in FAT32 format and with write caching disabled.
- USB 3.0 or above is recommended for use on the device.

NOTE: The USB data transfer function transfers only disturbance record files to USB key, the digital format setting file, event, alarm files can be transferred only by eSetup Easergy Pro.

The data is transferred to the USB key according to the following steps:

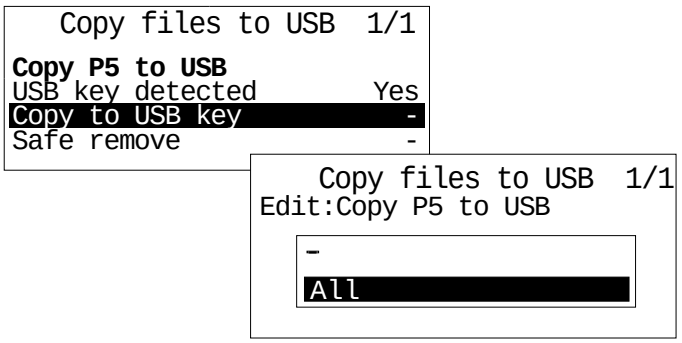
1. Use navigation keys to select and press OK key to enter **Device/Test** sub menu. Select **USB key** and press OK key to enter the view of **Copy files to USB**. Insert USB Key to the USB port in front of local panel.

   The **USB key detected** status will be changed from “No” to “Yes” automatically.



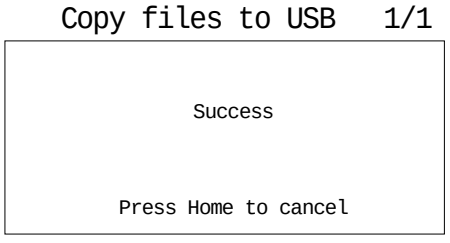
P533OKB

2. Press OK key to enable selection. Select **Copy to USB key** and then select **All** to copy all the files from the protection relay to USB key.



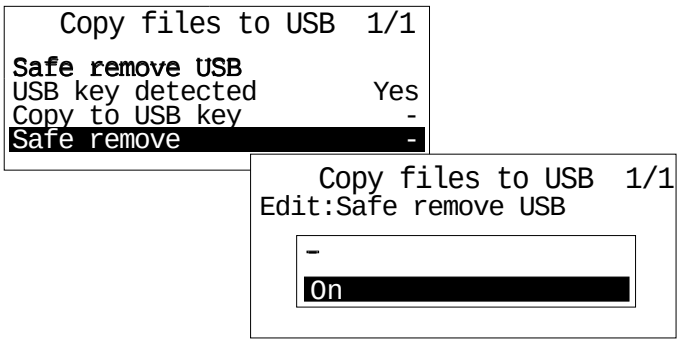
P533OJ02

3. A progress bar will be displayed on the screen for a short while. After finished copy, a “Success” message will be displayed. Please press ⌂ key to close this message.



P533O9B

4. To remove USB key, please select **Safe remove**, then select **On** and press OK key.



P533S0A

eSetup Easergy Pro

Overview

⚠WARNING

UNINTENDED EQUIPMENT OPERATION

Make sure that the reboot of the protection relay has no impact on people and equipment.

Failure to follow these instructions can result in death, serious injury, or equipment damage.

After changing some settings, the protection relay needs to reboot. During this time, the device is not operational.

eSetup Easergy Pro is a setting and operating software tool for configuring PowerLogic P5 devices, local operation and customisation functions.

The eSetup Easergy Pro software is supplied directly through the Schneider Electric website www.se.com, along with the eSetup Easergy Pro program for recovering disturbance recording files, and all the PowerLogic P5 documentation in PDF format.

Figure 189 - eSetup Easergy Pro menu bar and tool bar

The eSetup Easergy Pro software has a graphical interface where the protection relay settings and parameters are grouped under nine menu tabs:

- General
- Measurements
- Control
- Protection
- Matrix
- Logs
- Communication
- Device/Test
- Documentation
- Digital CB (optional)

The contents of the tabs depend on the device type and the selected application mode. Refer to the User Manual of eSetup Easergy Pro for detailed information on the setting views of each menu.

The eSetup Easergy Pro stores the device configuration in a setting file. The configuration of one physical device is saved in one setting file. The configurations can be printed out and saved for later use.

When starting to work with eSetup Easergy Pro, there are three options:

- Create a new setting file without connecting to a protection relay
- Open an existing (previously saved) setting file without connecting to a protection relay
- Connect to a relay and read the settings from the protection relay .

eSetup Easergy Pro can be connected to a single relay via the mini-USB port in the protection relay's local panel or to a group of protection relays through Ethernet.

Operation modes

The eSetup Easergy Pro software can be used in three operation modes:

- Disconnected mode
- Single unit connecting mode
- Network connecting mode

Using eSetup Easergy Pro in disconnected mode

The disconnected mode allows you to prepare parameters and settings files for PowerLogic P5 prior to commissioning.

The parameter and protection setting files prepared in disconnected mode will be downloaded later to the PowerLogic P5 protection relays in connected mode.

In this mode, the user can create a setting file from scratch, or open a previously saved setting file as a basis for creating configuration for a protection relay of the same type. Refer to the User Manual of eSetup Easergy Pro for more information.

Using eSetup Easergy Pro connected to a single PowerLogic P5

The single connection mode is used during commissioning of a PowerLogic P5 protection relay:

- To upload, download and modify PowerLogic P5 parameters and settings.

  Refer to the User Manual of eSetup Easergy Pro for more information on uploading (writing)/downloading (reading) setting files to/from the connected protection relays.

NOTICE

UNINTENDED EQUIPMENT OPERATION AND NUISANCE TRIPPING

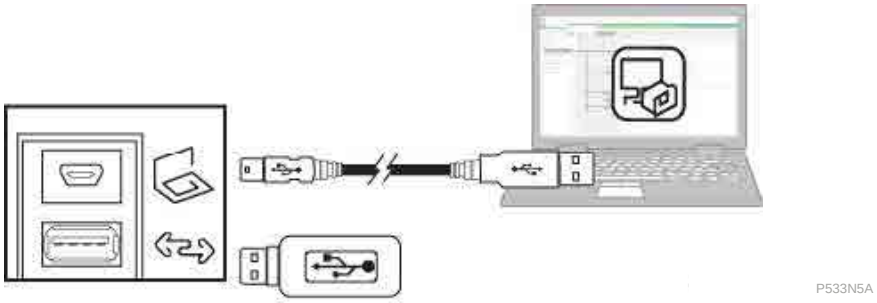
After writing new settings, configurations or firmware to a protection relay, perform a test to verify that the protection relay operates correctly with the new settings.

Failure to follow these instructions can result in unwanted shutdown of the electrical installation.

- To have all the measurements and supporting data available for commissioning.

The PC fitted with the eSetup Easergy Pro software is connected to the mini-USB port in the local panel of the PowerLogic P5 using a USB cord (reference 59700).

Figure 190 - Connecting a PC to the PowerLogic P5 using a USB cable



Using eSetup Easergy Pro connected to an PowerLogic P5 network

The network connection mode is used during operation:

- To manage the protection system.
- To check the status of the power supply.
- To diagnose any incident occurring on the power supply.

The PC fitted with the eSetup Easergy Pro software is connected to a group of PowerLogic P5 units via a communication network (connection via serial link or Ethernet).

The connection window allows configuration of the PowerLogic P5 network, and provides access to the parameter and protection setting files of the PowerLogic P5 units on the network.

Setting up the connection

Installing the USB driver

If it is the first time you connect the PowerLogic P5 protection relay to a PC running eSetup Easergy Pro, you need to install the USB driver on the PC.

The steps for installing the driver are as follows:

1. Connect the USB cable (reference 59700) to the front port of the PowerLogic P5 protection relay and the PC (see Connecting a PC to the PowerLogic P5 using a USB cable, page 258), after that look for a new COM port under COM & LPT in the Device Manager window of the PC.

   If you are unsure which is the right port, detach the USB cable and insert it again when you are in this menu.

2. Right-click on the port and select Update Driver Software from the contextual menu.

3. Select the option Browse my computer for driver software and locate the driver in the P5 driver_files folder under the eSetup Easergy Pro directory.

4. Click the Install button in the prompt window to start installing the driver.

5. If the driver has been installed successfully, the connection now appears under Network adapters in the Device Manager window each time you connect the PC to a PowerLogic P5 protection relay.

Connecting to a single protection relay using USB cable

1. Install the USB driver from the eSetup Easergy Pro file package for the first time connecting the PowerLogic P5 protection relay to a PC running eSetup Easergy Pro (see Installing the USB driver, page 259).
2. Connect the USB cable (reference 59700) between the PC running eSetup Easergy Pro and the local port of the PowerLogic P5 protection relay, with the mini-USB type B connector of the cable plugged into the protection relay and the type A connector to the PC (see Connecting a PC to the PowerLogic P5 using a USB cable, page 258).
3. On the eSetup Easergy Pro toolbar, click the **ON** connection button. The Login pop-up window opens.
4. Select the right PowerLogic P5 USB serial port name.
5. Click **Connect**.
   A new window showing the relay information opens.
6. Enter the user name and password to login.
   eSetup Easergy Pro's main view opens.

   NOTE: If you connect for the first time to a device on which the default users and passwords are used, refer to Cybersecurity, page 191.

Connecting to protection relays via Ethernet

You can connect to a single protection relay or multiple protection relays via Ethernet.

1. On the eSetup Easergy Pro toolbar, click the **ON** connection button. The Login pop-up window opens.
2. Click **ETHERNET**.
3. Select the right IP address from the drop-down menu.
   - For the protection relay's IP address, see the protection relay local panel menu **BUS**/**ETHERNET PORT**.
   - To save the defined connection settings, click the disk icon.
4. Click **Connect**. A new window showing the protection relay information opens.
5. Enter the user name and password to login. eSetup Easergy Pro's main view opens.

Web HMI

Overview

The web HMI is used for operation and settings. It has the same functions as eSetup Easergy Pro except the logic and mimic customisation.

The web HMI can be accessed using the following browsers[49][51]:

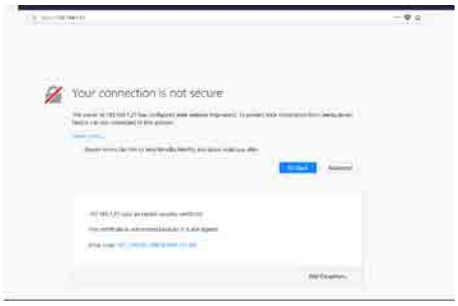
Operation system	Certificate state	Firefox®	Internet Explorer®	Edge®
Windows 7	without pre-installed certification	■	■	-
	pre-installed certification	■	■	-
Windows 10	without pre-installed certification	■	-	-
	pre-installed certification	■	■	■

Device reboot reminder

NOTE: Attention to the reminder message of device reboot.
Some setting changes require a reboot of the PowerLogic P5 protection relay. This is reminded by a message appearing on the HMI screen when you change such settings through the HMI.

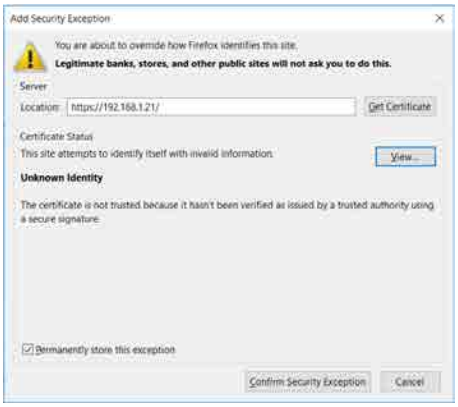
49. Chrome® is not supported.
50. Firefox is a registered trademark of the Mozilla Foundation.
51. Internet Explorer and Edge are registered trademarks of Microsoft Corporation.

Firefox



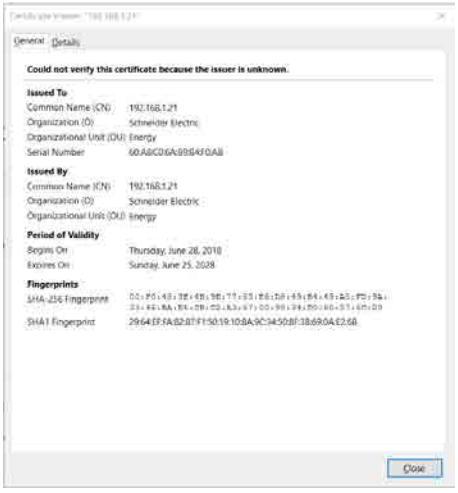
1. Enter "https://192.168.1.21" in the Firefox address bar, it will show the left message.

Click **Advanced** to show more information.



2. If a message regarding an invalid security certificate is displayed, click **Add Exception...**.

Left window will be displayed.



3. If needed, click the **View...** button to see the pop-up information of the certificate with the name "192.168.1.21.p12".

4. Close the certificate viewing window and then click the **Confirm Security Exception** button.

The login page will be opened.

5. Now the certificate file is already imported into Firefox and you find it in **Certificate Manager** of Firefox browser.

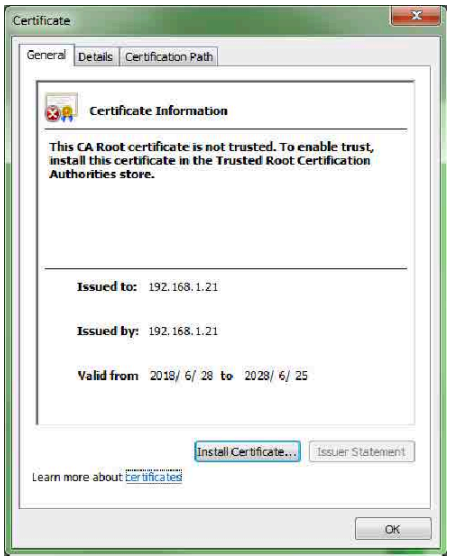
Internet Explorer in Windows 7

1. Enter "https://192.168.1.21" in the IE browser of Windows 7.

A warning messages window will pop-up.

2. Click **Continue to this website (not recommended)**.

Login page will be loaded with a "Certificate error" message displayed at the right end of address bar.

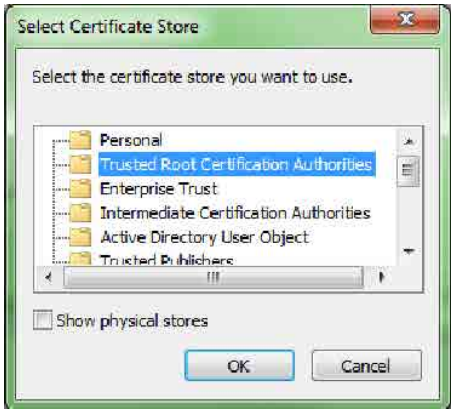


3. Click on **Certificate error** message, then click on **View certificates**.

There will be a pop-up window to show certificate information.

4. Click the **Install Certificate** button to install certificate.

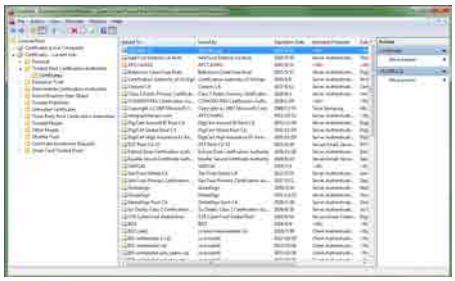
The "Certificate Import Wizard" window will be shown.



5. Click **Next**, on the **Certificate store** page, select the Certificate Store **Trusted Root Certification Authorities**.

6. Click **Finish** to import the certificate and close the Certificate Import Wizard window.

7. Click **Yes** on the pop-up Security Warning window to install the certificate.



8. The certificate is installed successfully and could be found under the Console Root/Certificates-Current User directory.

Edge in Windows 10

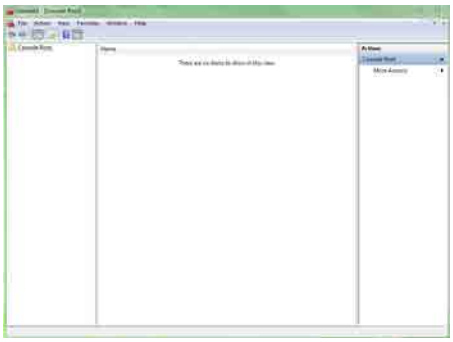
The following procedure for accessing the PowerLogic P5 web HMI uses the IE browser for illustration. The screen shots for the Edge browser are identical.

1. Enter "https://192.168.1.21" in the address bar of the Edge browser of Windows 10.

The left message will be displayed.

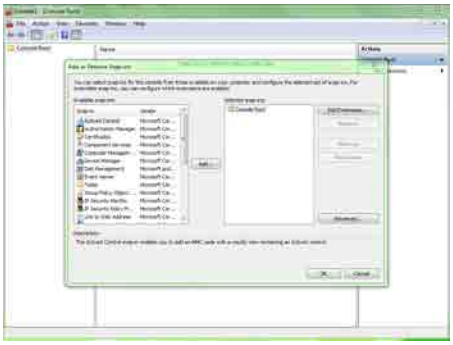
2. Click **Go on to the webpage (not recommended)**.

The left message displayed on the window, indicating that the right certificate needs to be installed in the computer first.



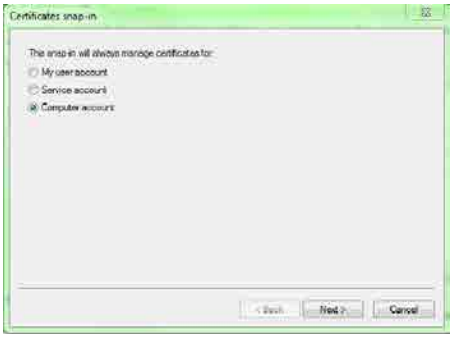
3. Click on **Start** button of desktop and then type in "mmc" in search bar.

The **Console** interface will be opened.



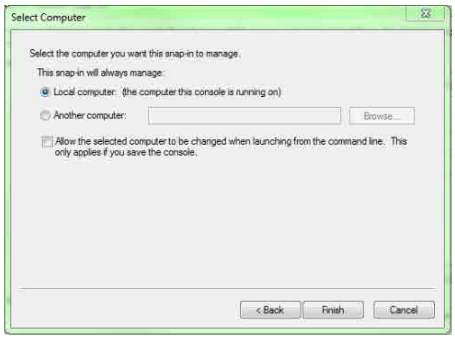
4. Click **File/Add/Remove Snap-in...**.

The **Add or Remove Snap-ins** window pops up.



5. Click **Certificates** in the left box and then click **Add** button.

The **Certificates Snap-in** window appears.

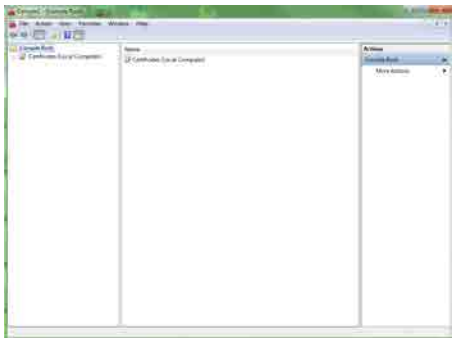


6. Select **Computer account** and click **Next**.

The **Select Computer** window appears.

7. Select **Local computer** and click **Finish** to close **Select computer** window.

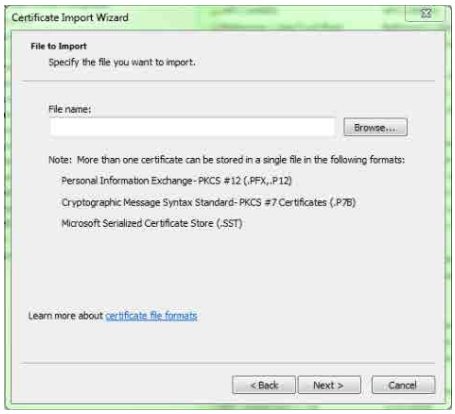
8. Click **Ok** to close **Add or Remove Snap-ins** window.



The “Console Root” folder in the **Console** interface is now populated with the "Certificates (local computer)" directory.

9. Select **Certificates (Local Computer)/Trusted Root Certification Authorities/Certificates** in the left box and then right click **Certificates** and select **All tasks/Import** in the context menu.

The "Certificate Import Wizard" window opens.

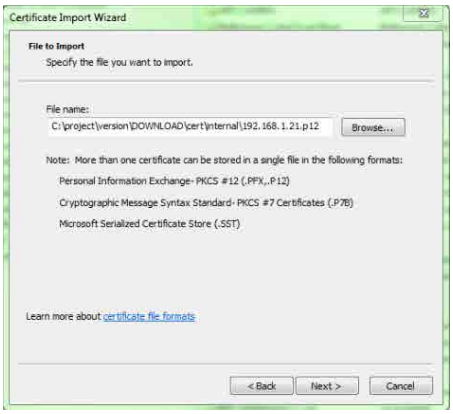


10. Click **Next**.

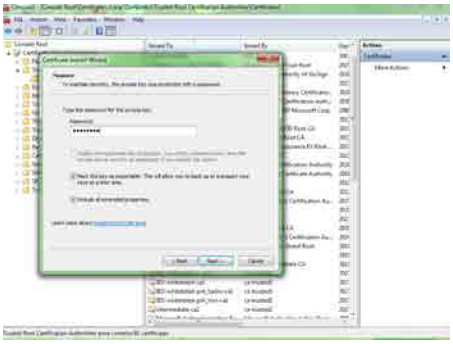
The "File to Import" window appears.

11. Click **Browse** and then, in the pop-up dialog box, select the path of the certificate followed by the certificate name "192.168.1.21.p12" (the suffix of the certificate is "p12").

Note that the file type should be **All Files**.

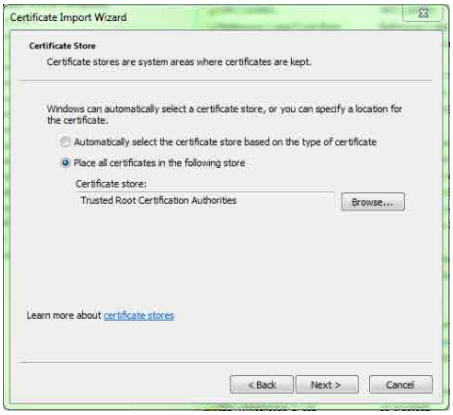


12. Click **Open** to finish locating the certificate file.



13. Click **Next** on the **File to Import** window.

The "Password" window appears.



14. Type in the password "secbrick", check the **Mark this key as exportable...** option, and then click **Next**.

The "Certificate Store" window appears.

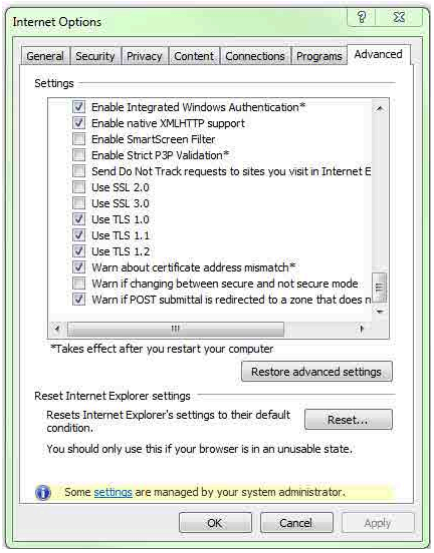
.

15. Check the **Place all certificates in the following store** option, browse to the certificate store folder "Trusted Root Certification Authorities", and then click **Next**.

The certificate import settings page appears.

16. Click **Finish**.

If the import is successful, a pop-up message with such content will appear on the screen.



17. After the certificate has been imported successfully, set up the Edge browser by checking the **Use TLS 1.0**, **Use TLS 1.1**, and **Use TLS 1.2** options under the **Advanced** tab of Internet options.

18. Enter "https://192.168.1.21" in the address bar of the Edge browser again.

Now we can access the Login page directly.

The EcoStruxure Power Device application

The EcoStruxure Power Device application is used to facilitate and simplify the operations and maintenance of the PowerLogic P5 protection relay, directly with a smart phone a few meters from the cubicle.

The EcoStruxure Power Device application can be connected to the PowerLogic P5 protection relay using a Wi-Fi router.

The EcoStruxure Power Device application provides easy access to device status, control and monitoring of the circuit breaker, measurements, settings, events and other functions through the mirror HMI or a simplified view.

- Mirror HMI:

  Duplicates the device display in the EcoStruxure Power Device application to perform actions more easily.

- Simplified view:

  The EcoStruxure Power Device application gives you an organised view of all the device's functionalities for easier access to data.

Connecting to protection relays via Ethernet

You can connect to a single protection relay or multiple protection relays via Ethernet.

Preparations before launching the EcoStruxure Power Device application

1. Equip the PowerLogic P5 protection relay with Ethernet modules (slot M or L).
2. Connect the PowerLogic P5 protection relay to a Wi-Fi router with RJ45 cable.
3. Configure the Wi-Fi network of the smart phone (IP address of the smart phone should be in the same network segment as the PowerLogic P5 protection relay).

Connecting to protection relays

1. Launch the EcoStruxure Power Device application.
2. Sign in with the account and password created at the Schneider Electric server.
3. Connect the new product via scanning QR code or selecting the PowerLogic P5 protection relay in the product list.
4. Enter the IP address of the PowerLogic P5 protection relay and click **Connect**.
5. Enter the username and password of the PowerLogic P5 protection relay.
6. A new window showing the PowerLogic P5 protection relay information opens.

Protection functions

General features of protection stages

Enable/disable protection functions

The different stages of the protection function can be enabled/disabled individually.

If a protection function stage is disabled, it is not shown in the **PROTECTION** menu in the local panel.

To enable or disable a protection function stage:

- With eSetup Easergy Pro or Web HMI, enter the **PROTECTION** menu/**Valid protection stages** sub-menu or directly go to each protection stage view in the same menu.
- With the local panel, enter the **Home** menu/**PROTECTION** sub-menu/**List of protection enabled** menu item/**Enabled Stages** menu item.

  The **Enabled Stages** menu item allows to enable or disable the protection stage(s) of a protection function. If a protection stage is enabled here, it appears in the **PROTECTION** menu as a menu option.

For the motor protection, there is a dedicated **Motor status** view (**PROTECTION** menu/**Motor status** sub-menu) where it is possible to enable or disable the following protection functions:

- Thermal overload protection for machine (ANSI code 49M)
- Motor start-up supervision (ANSI code 48)
- Motor restart inhibition (ANSI code 66)
- Locked rotor (ANSI code 51LR)
- Motor Anti-backspin (ABS) protection
- Motor speed detection
- Emergency restart

NOTE: The **Motor status** view is comprised of settings (e.g. nominal motor start current) common to these functions.

Setting groups

Setting groups are controlled by using controlling inputs like digital inputs, function keys, virtual inputs, HMI or custom logic.

When none of the assigned inputs are active, the active setting group is defined by parameter Setting group control in the **PROTECTION** menu/**Valid protection stages** sub-menu via eSetup Easergy Pro.

When one controlling input activates, the corresponding setting group is activated as well. If multiple inputs are active at the same time, the active setting group follows the definition by 'Setting group priority'.

By using virtual I/O the active setting group can be controlled using the local panel display, any communication protocol, or in-built programmable logic functions.

When a controlling input is configured, the **Setting group** parameter in the same menu is not operational.

Setting group changes are applied simultaneously to all protection functions.

Example of setting groups

Any digital input can be used to control setting groups but in this example DI1, DI2, DI3 and DI4 are chosen to control setting groups 1 to 4. This setting is done with the parameter 'Setting group x DI control' where x refers to the desired setting group.

'Setting group priority' is used to give a condition to a situation where two or more digital inputs, controlling setting groups, are active at the same time. 'Setting group priority' could have values: "1 to 4" or "4 to 1".

Assuming that DI2 and DI3 are active at the same time and 'Setting group priority' is set to "1 to 4" , setting group 2 becomes active. If 'Setting group priority' is reversed, that is, "4 to 1", the setting group 3 becomes active.

When a setting is selected by a digital input and this one is not activated, the 'Setting group' will not take effect.

Protection stage status

The status of a protection stage is one of the following:

- **Ok = '-'**

  The stage is idle and is measuring the analogue quantity for the protection. No power system fault detected.

- **Blocked**

  The stage is blocked for some reason (for example, through block matrix).

- **Start**

  The stage detected a fault (i.e. pick up value reached) and is counting the operation delay.

- **Trip**

  The stage has tripped and the fault is still on.

Directional operation

A global CT polarity setting is available in the **GENERAL** menu/**Scaling** submenu. These phase and neutral CT polarity settings affect:

- up to version v01.4xx.yyy only the ground differential protection function REF.

  NOTE: All other measurements and directional protection elements are not affected from this setting and still operate on measured current(s) and voltage(s) as per function description.

- from version v01.5xx.yyy additionally all measurements and directional protection elements (directional phase and neutral overcurrent, directional power, Wattmetric E/F, ...).

Mode of use for testing purposes

There is a **Mode of use** parameter which, when set to **Test** or **Test block** mode, allows forcing of the status of any protection stage to be **start** or **trip**. By using this forcing feature, current or voltage injection is not necessary to check the output matrix configuration, the wiring from the digital outputs to the circuit breaker and also to check that communication protocols are correctly transferring event information to a SCADA system.

The **Mode of use** can be configured in the **GENERAL** menu/**System info** sub-menu.

Start and trip signals

Every protection stage outputs two internal digital signals: start and trip. The start signal is issued when a fault has been detected. This start signal triggers the set operate timer. The trip signal is issued after the configured operate delay elapsed unless the fault disappears and starting resets before.

Global trip timer offers the possibility of assigning a dwell time delay (0.0...10.0 s) to the protection trip output. This **Minimum global trip cmd time** parameter can be configured in the **CONTROL** menu/**Global trip timer** sub-menu.

The hysteresis, as indicated in the protection stage's characteristics data, means that the signal is regarded as a fault until the signal drops below the start setting determined by the hysteresis value (see Hysteresis and reset ratio, page 275).

By using the output matrix, the user connects the internal start and trip signals to the digital outputs and indicators. See Output matrix, page 529.

Start and trip counters

Each protection function stage has a counter associated to the start and trip signals, they can be cleared individually.

Blocking

Any protection function, except arc-flash protection (see Arc-flash (ANSI 50ARC), page 388), can be blocked with internal and external signals through the block matrix. Internal signals are for example:

- logic outputs
- start signals from other stages
- trip signals from other stages

External signals are for example:

- digital inputs
- virtual inputs

Some protection stages are also inbuilt of blocking functions. For example, phase overcurrent protection with input of inrush detection.

Depending on the timing when the block input arrives at the protection function, the state of the protection will also be different:

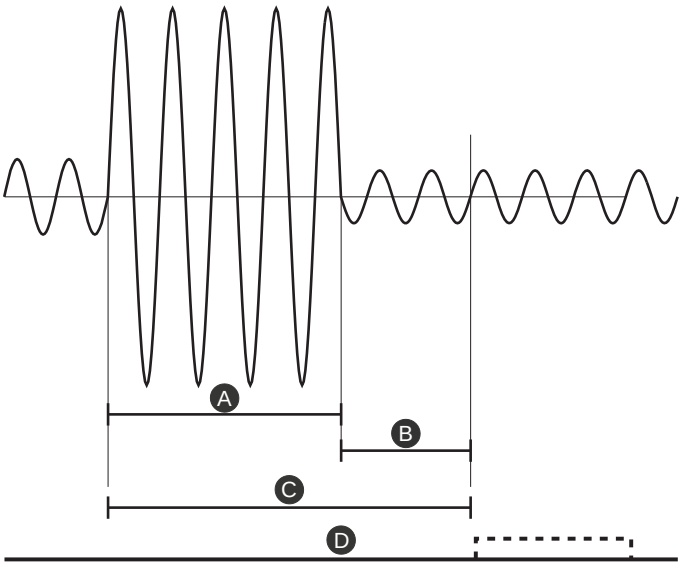
- If the protection is not started, the blocking input from block matrix will inhibit start, the protection will not trip in case of a fault condition.
- If the protection is started but not tripped, the blocking input from block matrix will freeze the delay counting until the blocking condition is off or the start resets, that is, the fault condition disappears.
- If the stage has already tripped, the blocking input from block matrix will reset both start and trip. The protection internal timer also resets to zero.

See Blocking matrix, page 529 for more information.

Overshoot time

Overshoot time is the time the protection relay needs to notice that a fault has been cleared during the operate time. This characteristic is important when grading the operate time settings between relays.

Figure 191 - Definition for overshoot time



A	Fault time	B	Overshoot time (≤ 50 ms)
C	Operate time configuration, have to be greater than the sum of fault time and overshoot time.	D	Trip contacts

For example, when there is a heavy fault in an outgoing feeder, it will start both the incoming and outgoing feeder relay. However, the fault must be cleared by the outgoing feeder protection relay and the incoming feeder relay must not trip. Although the operating delay setting of the incoming feeder is more than that of the outgoing feeder, the incoming feeder might still trip if the operate time difference is not big enough. The difference must be more than the overshoot time of the incoming feeder relay plus the operate time of the outgoing feeder circuit breaker.

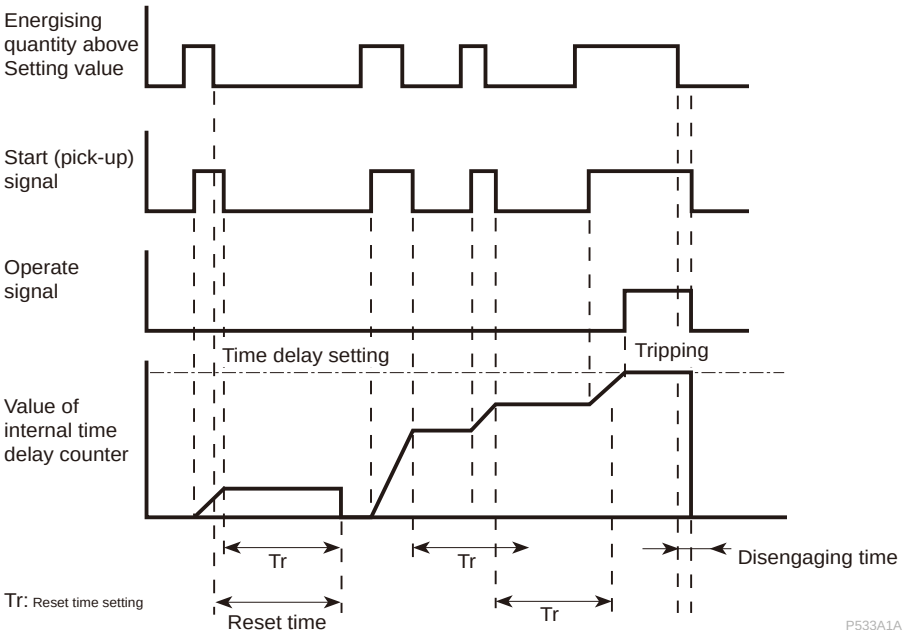
Definition for overshoot time, page 274 shows an overvoltage fault seen by the incoming feeder when the outgoing feeder clears the fault. If the operation delay setting would be slightly shorter or if the fault duration would be slightly longer than in the figure, an unselective trip might happen (the dashed pulse in the figure). In devices, the overshoot time is less than 50 ms.

Disengaging time and reset time

The disengaging time is the time between the moment when the fault conditions disappear and the moment the tripping contact relay opens. It is an instantaneous time.

Disengaging time and adjustable reset time according to IEC 60255-151 standard, page 275 shows an example of reset time, that is, release delay when the PowerLogic P5 protection relay is clearing an overcurrent fault. When the PowerLogic P5 protection relay's trip contacts are closed, the circuit breaker starts to open. After the circuit breaker contacts are open, the fault current still flows through an arc between the opened contacts. The current is finally cut off when the arc extinguishes at the next zero crossing of the current. This is the start moment of the reset delay. After the reset time delay the trip contact and start contact are opened unless latching is configured. The precise reset time depends on the fault size; after a significant fault, the reset time is longer. The reset time also depends on the specific protection stage. The maximum reset time for each stage is specified under the characteristics of every protection function.

Figure 192 - Disengaging time and adjustable reset time according to IEC 60255-151 standard



The adjustable reset time is a definite or inverse time hold used mainly to detect restriking faults (DT) or allow coordination with electromechanical protection relays (Inverse). It can be used also for coordination with electromechanical relays.

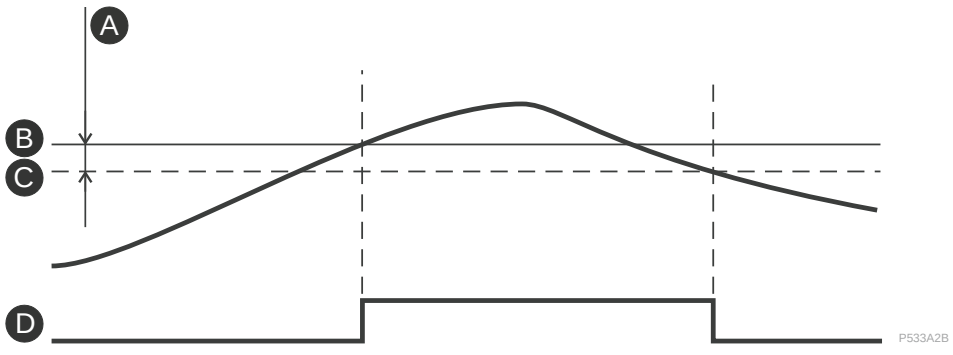
It is implemented in the following protection functions:

- Non-directional/directional phase overcurrent protection (ANSI 50/51/67)
- Non-directional/directional earth/ground fault overcurrent protection (ANSI 50N/51N/67N)
- Negative sequence overcurrent (ANSI 46)

Hysteresis and reset ratio

When comparing a measured value against a start value, some amount of hysteresis is needed to avoid oscillation near equilibrium situation. With zero hysteresis, any noise in the measured signal or any noise in the measurement itself would cause unwanted oscillation between fault-on and fault-off situations.

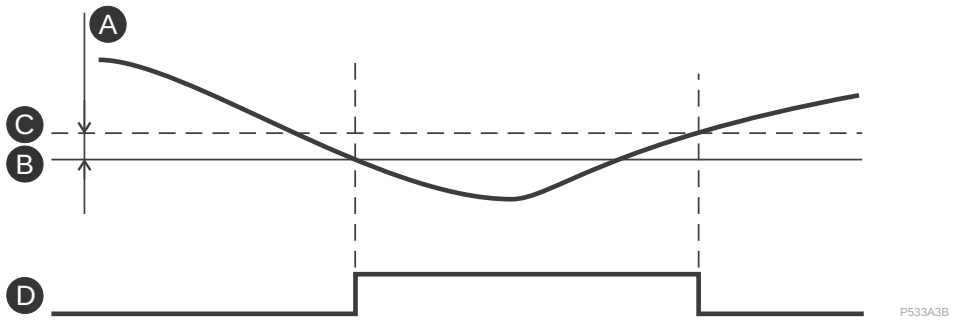
Figure 193 - Example of behaviour of an over-protection with hysteresis



A	Hysteresis	B	Start level
C	Reset level	D	Start

The reset ratio is the ratio between the reset level and the start level. To avoid any chattering of the protection for low settings of thresholds, a reset ratio can be claimed with a minimum value of hysteresis. For example: <93% with a minimum of hysteresis of 0.005 Inom.

Figure 194 - Example of behaviour of an under-protection with hysteresis



A	Hysteresis	B	Start level
C	Reset level	D	Start

Time grading for logic selectivity

When a fault occurs, the protection scheme only needs to trip circuit breakers whose operation is required to isolate the fault.

This selective tripping is also called discrimination or protection coordination and is typically achieved by time grading. Protection systems in successive zones are arranged to operate in times that are graded through the sequence of equipment so that upon the occurrence of a fault, although there are a number of protections that devices respond to, only those relevant to the faulty zone complete the tripping function.

The different operation time characteristics of control outputs have to be considered:

- the signaling of the raising edge (“make”) with high speed output is at least 5 ms faster than with conventional hinged-armature relay output;
- the signaling of the falling edge (“break”) with high speed output is at maximum 15 ms slower than with conventional hinged-armature relay output.

The recommended discrimination time between two PowerLogic P5 protection relays in an MV network is 200 ms considering a CB opening time of 60 ms.

Accuracy claims

All accuracy claims on operation and reset thresholds and times are based on tests performed according to related functional standard of the IEC 60255-1xx series.

Unless explicitly stated (or required per standard) the tests were executed under reference conditions:

- quasi-stationary semisolid signals at nominal frequency fnom (frequency protection excepted)
- total harmonic distortion ≤ 2 %
- ambient temperature 20°C (68°F)
- nominal auxiliary voltage VA.nom

Deviations are claimed relative to the setting under such reference conditions, where required also with an additional absolute value (usually relevant at very small/ low set thresholds only).

Recorded values on the last eight faults

There are detailed information available on the last eight faults for each of the protection stages. The recorded values are specific for protection stages and could contain information like time stamp, fault value, elapsed delay, fault current, fault voltage, phase angle and setting group.

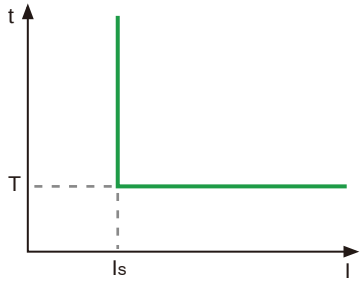
Dependent time and definite time operation

Description

Definite time protection

The tripping time is constant and gets triggered from the protection function starting.

Figure 195 - Definite time protection



Dependent time operation

The dependent time operation is the Inverse Definite Minimum Time (IDMT) type of operation in accordance with standards IEC 60255-151, BS 142 and IEEE C-37.112. The dependent time operation is available for several protection functions:

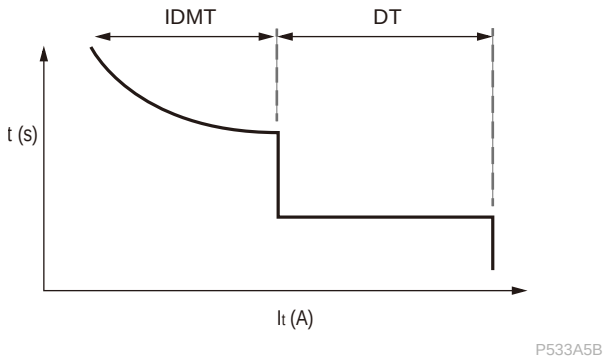
- Overcurrent protection (directional or not),
- Earth/ground fault protection (directional or not),
- Over/under voltage protection

The operate time in the dependent time mode (IDMT) is dependent on the magnitude of the fault. The bigger the fault, the faster the stage issues a trip signal and vice versa. The trip time calculation resets if the injected quantity drops below the start level.

The operate time in Definite Time (DT) mode is defined regardless of the fault signal. It is activated as soon as the pickup value is reached.

The operate time in the definite time mode is fixed by the operate delay setting. The timer starts when the protection stage starts and counts until the set time has elapsed. After that, the stage issues a trip command. If the fault is cleared before the definite time has elapsed, then the protection stage resets.

Figure 196 - Dependent time and definite time operation curves



Stage-specific dependent delay

Some protection functions have their own specific type of dependent delay. Details of these dedicated dependent delays are described with the appropriate protection function.

Operation modes

There are two operation modes to use the dependent time characteristics:

- Standard delays

  Using standard delay characteristics by selecting the **Operating curve** parameter in dedicated protection function. See Standard dependent operation delay, page 280.

- Fully programmable dependent delay characteristics

  Building the characteristics by setting 16 [current, time] points. The relay interpolates the values between given points with second degree polynomials. This mode is activated by the setting curve family to "PrgN", where N = 1, 2, 3, corresponding to the three different programmable curves available. Each programmed curve can be used independently by any number of protection stages. See Programmable dependent time curves, page 282.

Local panel graph

PowerLogic P5 protection relay shows a graph of the currently used dependent delay on the local panel display. The up and down keys can be used for zooming. Also the delays at 20 x I_{set}, 4 x I_{set}, 2 x I_{set} and 1.05 x I_{set} are shown.

Limitations

The minimum definite operation time starts when the measured value exceed the G_D[52] value, which is varied for different curves.

Curve	G_D (x G_S)
IEC SI	30
IEC VI	30
IEC EI	20
IEC LTI	30
UK RECT	15
RI	36
IEEE MI	76
IEEE VI	76
IEEE EI	76
NI CO8	76
STI CO2	76
LTI CO5	76
MI CO7	76
VI CO9	76
EI CO11	76
IEC UTI	76
FR STI	76

52. Threshold of independent time operation

BPN	76
ANSI NI	76
ANSI STI	76
ANSI LTI	76

Standard dependent operation delay

The standard dependent operation delay curves follow the equation below:

$$t(s) = TMS \times \left[\frac{k}{\left(\frac{G}{G_S} \right)^{\alpha} - p} + c \right]$$

P533OWB

where:

- t(s) is the operate time in seconds.
- G is the measured value.
- G_S is the start value.
- TMS is Time Multiplier Setting.

Table 50 - IDMT operating characteristics

Description **according to IEC60255-151 standard**	**k**	**c**	**α**	**p**	
Data attribute **according to IEC 61850-7-3 standard**	**setParA**	**setParB**	**setParC**	**setParD**	**SetCharact**
IEC Standard Inverse (IEC/A)	0.14	0	0.02	1	9
IEC Very Inverse (IEC/B)	13.5	0	1	1	10
IEC Extremely Inverse (IEC/C)	80	0	2	1	12
IEC Long Time Inverse	120	0	1	1	14
IEC Ultra Time Inverse	315.2	0	2.1	1	17
Rectifier Inverse	45900	0	5.6	1	18
RI	-4.2373	0	-1	1.43644	19
FR Short Time Inverse	0.05	0	0.04	1	20
BPN (EDF)	1000	0.655	2	1	21
IEEE Moderately Inverse (IEC/D)	0.0515	0.114	0.02	1	4
IEEE Very Inverse (IEC/E)	19.61	0.491	2	1	2
IEEE Extremely Inverse (IEC/F)	28.2	0.1217	2	1	1
Short-Time Inverse (CO2)	0.1052	0.0262	0.8	1	22

Table 50 - IDMT operating characteristics (Continued)

Description according to IEC60255-151 standard	k	c	α	p	
Data attribute according to IEC 61850-7-3 standard	setParA	setParB	setParC	setParD	SetCharact
Long-Time Inverse (CO5)	4.842	1.967	1.1	1	23
Moderately Inverse (CO7)	0.0094	0.0366	0.02	1	24
Inverse (CO8)	5.95	0.18	2	1	25
Very Inverse (CO9)	4.12	0.0958	2	1	26
Extremely Inverse (CO11)	5.57	0.028	2	1	27
ANSI Normally Inverse	8.9341	0.17966	2.0938	1	29
ANSI Short Time Inverse	0.2663	0.03393	1.2969	1	30
ANSI Long Time Inverse	5.6143	2.18592	1	1	31

NOTE:

- SetCharact is for DT curve: 5.
- The effective operate value is greater than G_S.

Standard dependent reset delay

After the IDMT time elapses, the operation timer is reset when the start signal goes low, according to the following equation:

$$t_{reset}(I) = TMS \times \left[\frac{tr}{1 - \left(\frac{G}{G_s} \right)^{p}} \right]$$

P533OXB

The reset time characteristic is defined by a setting in the protection stage. The allowed settings are dependent on the operate curve as shown in the table.

Table 51 - IDMT reset time

Operating curve	Reset curve		
	IDMT		DT
	tr(s)	P	
DT	-	-	Yes
IEC Standard Inverse (IEC/A)	8.2	6.45	Yes
IEC Very Inverse (IEC/B)	50.92	2.4	Yes
IEC Extremely Inverse (IEC/C)	44.1	3.03	Yes
IEC Long Time Inverse)	40.62	0.4	Yes
IEC Ultra Time Inverse	-	-	Yes
Rectifier Inverse	-	-	Yes

Table 51 - IDMT reset time (Continued)

Operating curve	Reset curve		
	IDMT		DT
	tr(s)	P	
RI	-	-	Yes
FR Short Time Inverse	-	-	Yes
BPN (EDF)	-	-	Yes
IEEE Moderately Inverse (IEC/D)	4.85	2	Yes
IEEE Very Inverse (IEC/E)	21.6	2	Yes
IEEE Extremely Inverse (IEC/F)	29.1	2	Yes
Short-Time Inverse (CO2)	0.1052	2	Yes
Long-Time Inverse (CO5)	4.842	2	Yes
Moderately Inverse (CO7)	0.0094	2	Yes
Inverse (CO8)	5.95	2	Yes
Very Inverse (CO9)	4.12	2	Yes
Extremely Inverse (CO11)	5.57	2	Yes
ANSI Normally Inverse	9	2	Yes
ANSI Short Time Inverse	0.5	2	Yes
ANSI Long Time Inverse	15.75	2	Yes

The TMS (inverse time coefficient) of the IDMT reset curve is the one defined for the operating curve.

For all operating curves not listed in the table above, the reset curve is of DT type.

Programmable dependent time curves

Programming dependent time curves requires eSetup Easergy Pro setting tool and rebooting the unit.

The [current, time] curve points are programmed using eSetup Easergy Pro PC program. There are some rules for defining the curve points:

- the configuration must begin from the top line
- the line order must be as follows: the smallest current (longest operate time) on the top and the largest current (shortest operate time) on the bottom
- all unused lines (on the bottom) should be filled with I/I_{start} = 1 and operate time = 0.00 s

Here is an example configuration of curve points:

Table 52 - Example configuration of curve points

Point	Current I/I_{start}	Operate delay
1	1.00	10.00 s
2	2.00	6.50 s
3	5.00	4.00 s
4	10.00	3.00 s
5	20.00	2.00 s
6	40.00	1.00 s
7	1.00	0.00 s
8	1.00	0.00 s

Table 52 - Example configuration of curve points (Continued)

Point	Current I/I_{start}	Operate delay
9	1.00	0.00 s
10	1.00	0.00 s
11	1.00	0.00 s
12	1.00	0.00 s
13	1.00	0.00 s
14	1.00	0.00 s
15	1.00	0.00 s
16	1.00	0.00 s

Cold load pick-up

Description

Cold load pick-up

The cold load pickup function detects that a cold load condition exists and provides an information to optionally change the selected current protection settings for defined duration of time after energisation of the load.

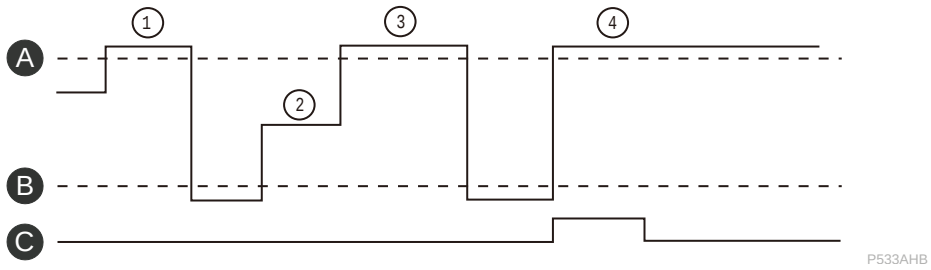
A situation is regarded as cold load when all the three phase currents have been below a given idle value for longer than the cold time setting and then at least one of the currents exceeds a given pick-up level within 80 ms. In such a case, the cold load detection signal is activated and will keep active for "CLPU time delay" for a given time. This signal is available for the output matrix and blocking matrix.

Application for cold load detection

Right after closing a circuit breaker, a given amount of overload can be allowed for a given limited time to take care of situations where a load has been de-energised for an extended period of time and is then re-energised. This applies particularly to applications such as motor loads (e.g., compressor motor inside air conditioning loads) or thermostatically controlled heating of water where the load current is much greater for a cold load than when it is operating normally. So, the cold load pickup function can improve the profiling of overcurrent protection settings to dynamic load situations caused by load de-energisation.

Example

Figure 197 - Functionality of cold load current feature



A	Pick-up value	B	Idle state
C	Cold load		

1. No activation because the current has not been under the set Idle current.
2. Current dropped under the Idle current level but now it stays between the Idle current and the pick-up current for over 80 ms.
3. No activation because the phase two lasted longer than 80 ms.
4. Now we have a cold load activation which lasts as long as the “CLPU time delay” was set or as long as the current stays above the pick-up setting.

Characteristics

Table 53 - Settings and characteristics of cold load pick-up function

Settings/characteristics (description/label)	Value
Idle current/Idle current	
Range	0.01...0.50 pu[53]
Resolution	0.01 pu[53]
Pickup current/Pickup	
Range	0.30...10.00 pu[53]
Resolution	0.01 pu[53]
CLPU dead time/Dead time	
Setting range	0.10...14400.00 s
Resolution	0.01 s
CLPU time delay/Max time	
Setting range	0.01...300.00 s
Resolution	0.01 s
Accuracy	1% or ±20 ms

53. Nominal CT Rating

Selective Overcurrent Logic (SOL)

Description

The Selective Overcurrent Logic (SOL) function, can considerably reduce the tripping time of the circuit breakers closest to the source, compared to a pure time discrimination, and may be used for logic discrimination in closed ring networks also using directional protection.

SOL function is applied to the non-directional/directional phase overcurrent protection (ANSI 50/51/67), non-directional/directional earth/ground fault overcurrent protection (ANSI 50N/51N/50G/51G/67N), definite time and IDMT.

With PowerLogic P5 protection relays, the discrimination can be done in two different ways:

- Logic overcurrent stages protection functions that send SOL signals (downstream protection) and that may be prevented from tripping by the reception of SOL signals (upstream protection).
- Time-based overcurrent stages: protection stages that may delayed by SOL signals (upstream protection). They are used as backup for the logic overcurrent stages.

When a fault occurs:

- Any downstream protection can activate the SOL function through the output matrix, so that the SOL function can send a SOL signal to the upstream protections.
- At the reception of the SOL signal by the upstream protection, the latter changes its operating delay from operate delay to SOL operate delay. When the upstream protection is using IDMT delay, SOL will also have impact on the curve settings.

Operation

To implement the SOL function, downstream and upstream protection should be set as follows:

Set the downstream protection to send the SOL1 trip signal to upstream relay:

1. Check the **Enable for SOL** box in the **Selective overcurrent logic** view of **PROTECTION** Menu in Easergy Pro.
2. Select from the drop-down list of **SOL signal number**.
3. Set the value of **CB trip clearing time**.
4. Switch to **MATRIX** menu/**Output matrix** submenu, configure the PowerLogic P5 output matrix:

   Connect the start signals of the different protections involved in the logic discrimination to the SOLxStart (x = 1 or 2) signal, then connect the SOLx trip (x = 1 or 2) signal to a dedicated contact relay or GOOSE output.

Set the upstream protection to receive the SOLx trip signal:

1. Configure the PowerLogic P5 output matrix:

   Connect the dedicated logic input (DI or GOOSE input signal), linked with the downstream SOLx trip signal, to the SOL Inputx signal.
2. Switch to **PROTECTION** menu, select specific protection function in the left column, set the SOL status to the value "SOLx"
3. Set the **SOL operate delay** to a value higher than the value of the setting **Operate delay**.

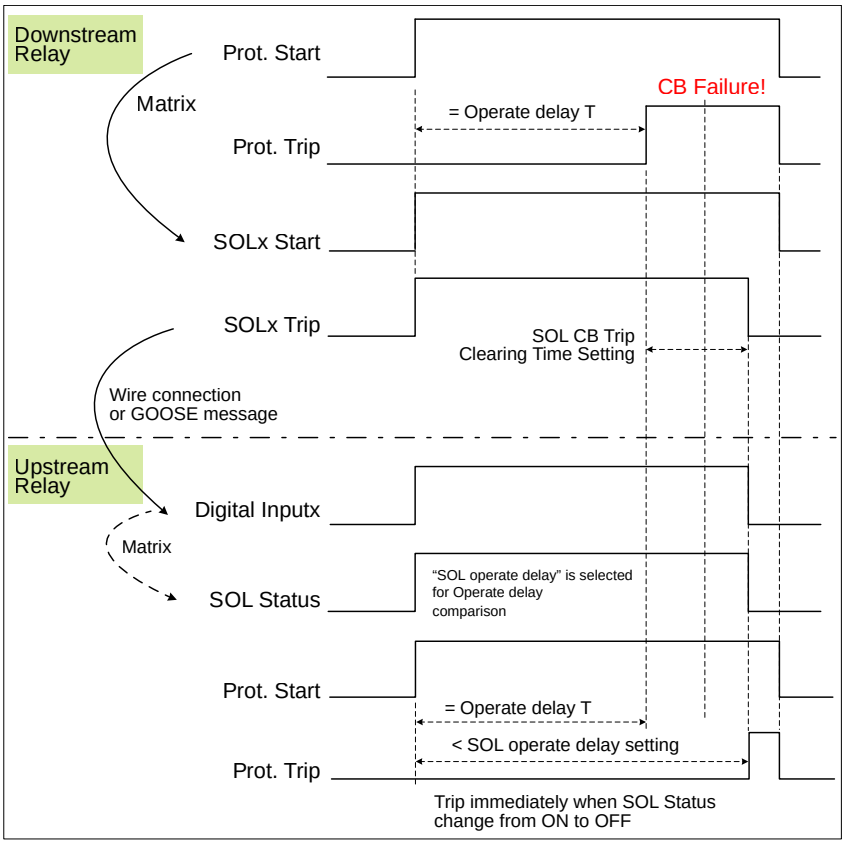
Up to two output signals can be provided by the SOL function.

The value of the setting **SOL operate delay** should be greater than the value of the setting **Operate delay** in the overcurrent protection plus the value of the setting **CB trip clearing time** in the SOL function. The setting **SOL operate delay**

can make sure the downstream protection tripping with selectivity. The setting **CB trip clearing time** is used to set the release time of the SOL trip signal for the downstream protection.

If a fault occurs at downstream, the downstream protection issues a trip command to isolate the fault according to the value of the setting **Operate delay**. Then a global trip signal is activated by the trip signal. At the same time, a timer with the value of the setting **CB trip clearing time** is triggered by the global trip signal and starts timing. If the downstream protection successfully isolates the fault, the SOL signal is released and all the P5 relays of the upstream protection will be reset. If the downstream protection cannot clear the fault due to a circuit breaker fail, when the tripping duration time of the downstream protection exceeds the value of the setting **CB trip clearing time**, consequently upstream protection nearest to the downstream protection will switch the value of the setting **SOL operate delay** to the value of the setting **Operate delay** due to no reception of the SOL signal. Then the protection will trip immediately.

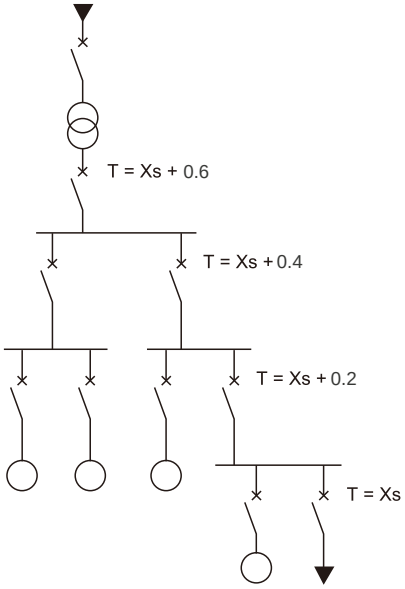
The SOL operate delay of the upstream protection usually takes into account the breaking device operating time and the protection reset time.



NOTE: Normally Prot.Start/Prot.Trip means the start/trip signal of over current protection or earth/ground fault protection (50/51/67/50N/51N/50G/51G/67N). SOL operation delay setting should be greater than "Operation delay T + SOL CB Trip Clearing Time Setting".

Example 1

Figure 198 - Example 1: Radial distribution with use of time-based discrimination

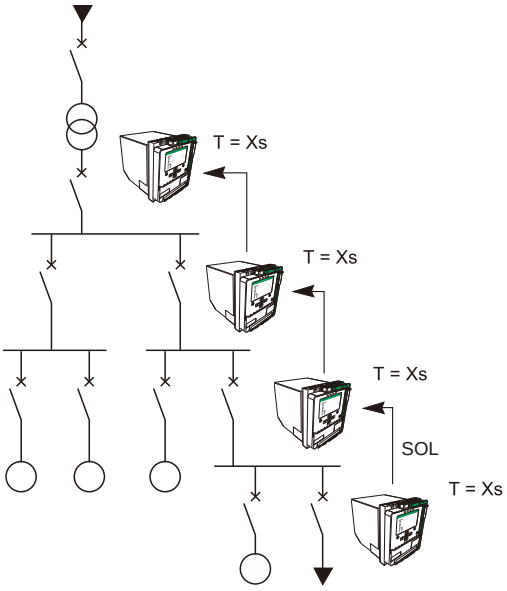


T: operate delay setting in protection function

The upstream protection units are typically delayed by 0.2 s to give the downstream protection units time to trip. When there are many levels of discrimination, the protection tripping time at the source is long. In this example, if the protection tripping time for the protection unit furthest downstream is Xs = 0.2 s, the protection tripping time at the source is T = Xs + 0.6 s = 0.8 s.

Example 2

Figure 199 - Example 2: Radial distribution with use of logic discrimination

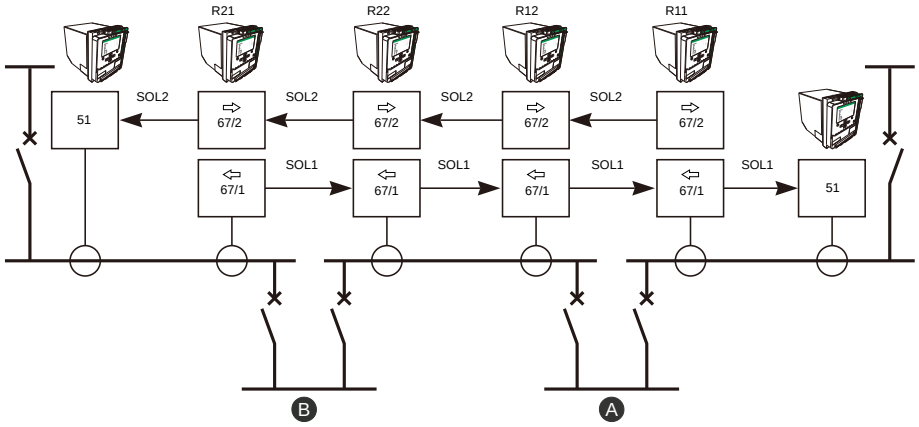


T: operate delay setting in protection function

When a fault appears, the protection units that detect it inhibit the upstream protection units by switching to the SOL operate delay setting. The protection unit furthest downstream trips since it is not blocked by another protection unit. The delays are to be set in accordance with the device to be protected.

Closed ring network application

The SOL function can support the closed ring network which includes two substations application, each of which comprises two PowerLogic P5 relays, marked R11, R12 and R21, R22. Each of the PowerLogic P5 relay configures different directional overcurrent units (stages).



A Substation 1 B Substation 2

Starting at one end of the ring, the detection direction of PowerLogic P5 unit 1 and 2 of the directional protection functions should be alternated between line and busbars.

Characteristics

Settings and characteristics	Values
Enable for SOL/SOL	
Options[54]	Disabled; Enabled
SOL1Start	
Options[54]	-; Trip
SOL2Start	
Options[54]	-; Trip
SOL signal number/SOL op number	
Range	1, 2
CB trip clearing time/CB trip time	
Setting range	0.00...1.00 s
Resolution	0.01 s

54. Configured via Output Matrix

Incomer fault locator (ANSI 21FL)

Description

The PowerLogic P5 protection relay can locate a short-circuit in a radial operated network.

The fault location is given in reactance (ohms) and kilometers or miles. The fault value can then be exported, for example, with an event to a Distribution Management System (DMS). The system can then localise the fault. If a DMS is not available, the distance to the fault is displayed as kilometers, and as a reactance value. However, the distance value is valid only if the line reactance is set correctly. Furthermore, the line should be homogenous, that is, the wire type of the line should be the same for the whole length. If there are several wire types on the same line, an average line reactance value can be used to get an approximate distance value to the fault. Names and reactance values for widely used overhead wires are:

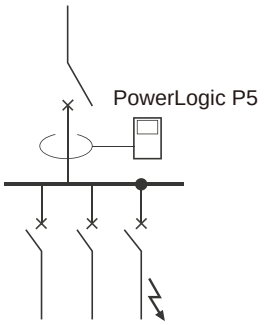
- Sparrow: 0.408 ohms/km or 0.656 ohms/mile
- Raven: 0.378 ohms/km or 0.608 ohms/mile

NOTE: The fault locator is normally used in the incoming bay of the substation. Therefore, the fault location is obtained for the whole network with just one PowerLogic P5 protection relay, by compensating the effect of the healthy feeders.

The incomer short circuit fault locator operates if:

- The PowerLogic P5 protection relay is located in the incoming feeder.
- The CTs and VTs are connected such that the fault is seen in the forwards direction. Any fault seen in the reverse direction will not produce a fault location result.

Figure 200 - Example of fault on feeder detected by the incomer fault detector



The algorithm functions in the following order:

1. The needed measurements (phase currents and phase to phase voltages) are continuously available.
2. The fault distance calculation can be triggered in two ways:
   - By opening a feeder circuit breaker due to a fault and sudden increase in phase currents (Enable incomer fault locator + Triggering digital input).
   - Another option is to use only the sudden increase in the phase currents (Enable incomer fault locator).
3. Phase currents and voltages are registered in three stages: before the fault, during the fault and after the faulty feeder circuit breaker was opened.
4. The fault distance quantities are calculated.
5. Two phases with the biggest fault current are selected.
6. The load currents are compensated.
7. The faulty line length reactance is calculated.

$$Z_{AB} = \frac{\vec{V}_A - \vec{V}_B}{\vec{I}_A - \vec{I}_B - \vec{I}_{pre\text{-}fault}}$$

P533AKB

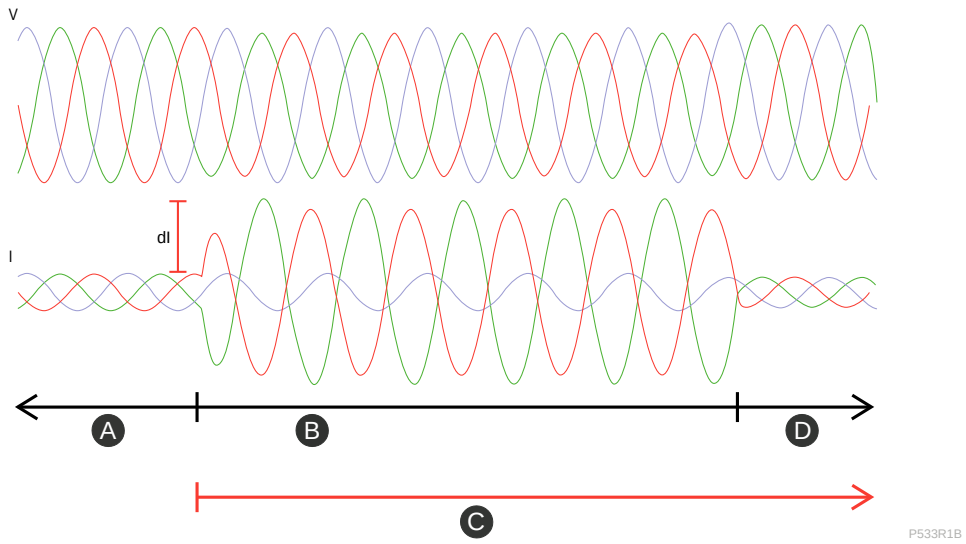
VA	Phase A to ground voltage
VB	Phase B to ground voltage
IA	Phase A current
IB	Phase B current
$I_{pre\text{-}fault}$	Pre-fault load current

The reference current setting is used to start the calculation of the fault locator based on the pre-fault current magnitude. The calculation can be triggered by a digital or logic input.

Example

An application example where the fault location algorithm is used at the incomer side is presented below. The settings of the Incomer fault locator function is configured in the **PROTECTION** menu/**Incomer fault locator** sub-menu.

Figure 201 - Illustration of the fault location algorithm used at the incomer side



P533R1B

A	Pre-fault time more than 2 s	B	In order to calculate the fault location, the fault current must be present for at least 0.08 s and last no longer than 1 s
C	When the digital input is used together with the current change, the input signal has to be activated at least 0.5 s after the fault occurs	D	Post-fault only few cycles

Characteristics

Table 54 - Setting parameters of incomer fault locator

Parameter	Value	Unit	Default	Description
Triggering digital input (Trig DI)	Selection of one digital input (DI), one virtual input (VI), one virtual output (VO), or one function key (Fx)	-	-	Trigger mode (= triggering based on sudden increase of phase current, otherwise sudden increase of phase current + DIx/VIx)
Line reactance/ unit (Xline)	0.010...10.000	Ohm	0.389	Per unit (positive-sequence) reactance of the line. This value is only used to convert the fault reactance to the distance per set unit (kilometers or miles).
Current change to trig (dI)	0.10...8.00	pu	0.5	Trig current (sudden increase of phase current)
Blocked before next trig	10...600	s	70	Blocks function for this time after trigger. This is used for blocking calculation during auto-reclosing sequences.
Xmax limit	0.5...500.0	Ohm	500.0	Limit for maximum reactance. If the reactance value is above the set limit, the calculation result is not shown.
Unit	Editable for user	-	km	-
Event	Disabled; Enabled	-	Enabled	Event mask
Accept zero pre-fault current	Disabled; Enabled	-	Disabled	-

Table 55 - Measured and recorded values of incomer short circuit fault locator

	Parameter	Unit	Description
Measured values/ recorded values	Distance fault	km	Distance to fault
	XFlt	Ohm	Fault reactance
	Date	-	Fault date
	Time	hh:mm:ss:mss	Fault time
	Cntr	-	Number of faults
	Pre	A	Current before fault (= load current)
	Fault	A	Fault current
	Post	A	Current after fault
	V drop	%	Voltage drop during the fault
	Duration	s	Fault duration
	Type	-	Fault type (1-2, 2-3, 1-3, 1-2-3)

Feeder fault locator (ANSI 21FL)

Description

The PowerLogic P5 protection relay can locate a short-circuit fault and an earth/ground fault on the feeder itself in a radially operated network. The fault location function (ANSI code 21FL) is given as a reactance (ohms) and converted to kilometers or miles. The fault value can then be exported, for example, with an event to a Distribution Management System (DMS). The system can then localise the fault. If a DMS is not available, the distance to the fault is displayed as kilometers/miles and as a reactance value.

However, the distance value is valid only if the line reactance is set correctly.

Furthermore, the line should be homogenous, that is, the wire type of the line should be the same for the whole length. If there are several wire types on the same line, an average line reactance value can be used to get an approximate distance value to the fault. Names and reactance values for widely used overhead wires are:

- Sparrow: 0.408 ohms/km or 0.656 ohms/mile
- Raven: 0.378 ohms/km or 0.608 ohms/mile

When the feeder fault locator is calculating short-circuit impedance, the following formula is used:

$$\vec{Z}_{AB} = \frac{\vec{V}_A - \vec{V}_B}{\vec{I}_A - \vec{I}_B}$$

P533ANB

VA	Phase A to ground voltage
VB	Phase B to ground voltage
IA	Phase A current
IB	Phase B current

When the feeder fault locator is calculating ground fault impedance, the following is used (e.g. for phase A):

$$\vec{Z}_A = \frac{\vec{V}_A}{\vec{I}_A + k \times \vec{I}_N}$$

P533APB

VA	Phase A to ground voltage
IA	Phase A current
k	Earth/ground factor k, needs to be set by user
IN	Earth/ground fault overcurrent, calculated from phase currents (IN.calc)

$$\overrightarrow{IN}_{.calc} = \vec{I}_A + \vec{I}_B + \vec{I}_C$$

P533ARB

The earth/ground factor k is calculated with the following formula:

$k = (Z_{0L} - Z_{1L}) / (3 \times Z_{1L})$

where:

Z_{0L} = Zero sequence line impedance

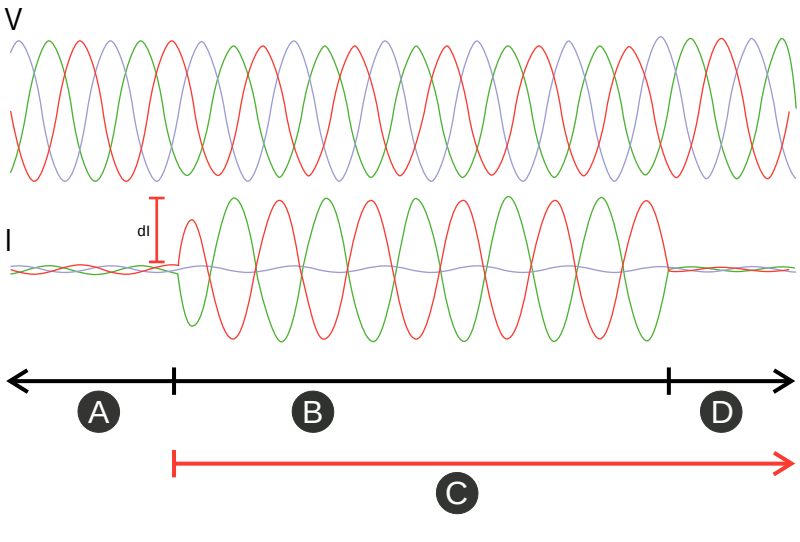
Z_{1L} = Positive sequence line impedance

Fault reactance calculation is triggered if the start value is exceeded or both “Start setting” and “Triggering digital input” terms are fulfilled. When used, “Triggering digital input” can be either digital or virtual input.

Example

An application example where the fault location algorithm is used at the feeder side is presented below. The settings of the feeder fault locator function is configured in the **PROTECTION** menu/**Feeder fault locator** sub-menu.

Figure 202 - Illustration of the fault location algorithm used at the feeder side



A	Pre-fault time more than 2 s	B	In order to calculate the fault location the fault current must be present for at least 0.08 s and last no longer than 1 s
C	When the digital input is used together with the current change, the input signal has to be activated at least 0.5 s after the fault occurs	D	Post-fault only few cycles

Characteristics

Table 56 - Settings and characteristics of the feeder fault locator function (ANSI 21FL)

Parameter	Value	Unit	Default	Description
Pick-up value	0.10...5.00	pu[55]	1.2	Current limit for triggering.
Triggering digital input	Selection of one digital input (DI), one virtual input (VI), one virtual output (VO), or one function key (Fx)	-	-	Trigger mode (= triggering based on sudden increase of phase current, otherwise sudden increase of phase current + DIx/VIx/VOx/Fx)
Line reactance/ unit (Xline)	0.010...10.000	Ohm	0.491	Per unit positive-sequence reactance of the line. This value is only used to convert the fault reactance to the distance per set unit (kilometers or miles).
Earth factor	0.000...10.000	-	0.678	Calculated earth factor from line specifications.
Earth factor angle	-60... +60	°	10	Angle of calculated earth factor from line specifications.
Unit	km	-	km	Unit of distance
Event enabling	Off; On	-	On	Event mask

55. Inom = phase CT primary nominal

Table 57 - Measured and recorded values of feeder fault locator

	Parameter	Unit	Description
Measured values/ recorded values	Distance	km	Distance to the fault
	Xfault	Ohm	Fault reactance
	Cntr	-	Number of faults
	Type	-	Fault type: IA-N, IB-N, IC-N; IA, IB-N; IB, IC-N; IA, IC-N; IA-IB; IB-IC; IA-IC IA-B-C; IA, B, C-N

Neutral admittance (ANSI 21YN)

Description

The neutral admittance protection function can be applied in high resistance earthed/grounded, unearthed/ungrounded or compensated power system to detect earth/ground fault with increased sensitivity. Two stages of the neutral admittance protection are available in the PowerLogic P5 protection relay, each stage has three elements: over-admittance (YN>1 or YN>2), over-conductance (GN > 1 or GN > 2) and over- susceptance (BN > 1 or BN > 2).

The neutral admittance Y_n is calculated based on the neutral current IN and the neutral voltage VN:

$Y_n = G_n + jB_n = IN / -VN = 3IN / -3VN$

The source of the neutral current is settable from the sensitive E/F CT, CSH core balance CT, standard E/F CT, or the sum of three phase currents.

The neutral admittance protection is blocked if the following conditions are met:

- The neutral current is based on the sum of three phase currents
- The CTS supervision function detects a CT failure
- The CTS output signal is configured to block neutral admittance protection through the blocking matrix

The source of the neutral voltage is from the direct measurement when the Voltage mode is “+VN”, otherwise the source of the neutral voltage is from the sum of three phase voltages. The neutral admittance protection is only active when the neutral voltage VN is above the setting threshold.

The neutral admittance protection is also blocked if the following conditions are met:

- The neutral voltage is based on the sum of three phase voltages
- The VTS supervision function detects a VT failure
- The VTS output signal is configured to block neutral admittance protection through the blocking matrix

The settings of the admittance protection are based on the percentage of the rated neutral admittance. The formula for calculating the rated neutral admittance are listed in the table below.

Table 58 - Calculation of the rated neutral admittance

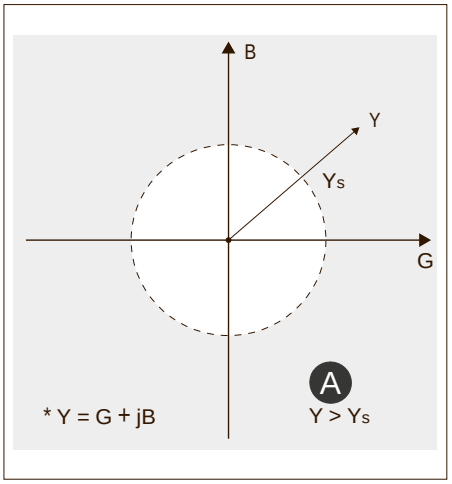
IN source	VN source	Rated neutral admittance (Y_n)
Sensitive E/F CT	VN	Sensitive IN CT primary / (√3*VN primary)
Sensitive E/F CT	(VA + VB + VC)	Sensitive IN CT primary / (√3*VT primary)
CSH core balance CT	VN	Nominal IN.CSH / (√3*VN primary)
CSH core balance CT	(VA + VB + VC)	Nominal IN.CSH / (√3*VT primary)
Standard E/F CT	VN	EF CT primary / (√3*VN primary)
Standard E/F CT	(VA + VB + VC)	EF CT primary / (√3*VT primary)
(IA + IB + IC)	VN	CT primary / (√3*VN primary)
(IA + IB + IC)	(VA + VB + VC)	CT primary / (√3*VT primary)

Operation

Operation of admittance protection

The admittance protection is non-directional. Hence, provided the magnitude of admittance exceeds the set value YN>1, the protection relay will operate.

Figure 203 - Admittance protection operation with non-directional characteristic

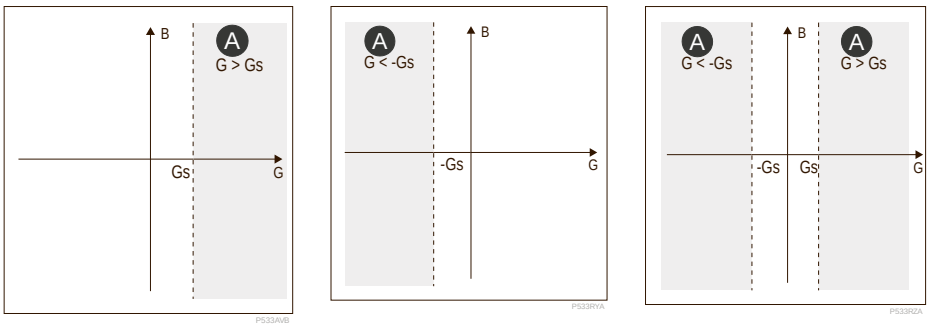


A Operate zone

Operation of conductance protection

The conductance protection may be set to non-directional, forward or reverse. Hence, provided the magnitude and the directional criteria are met for conductance, the PowerLogic P5 protection relay will operate. The correction angle causes rotation of the directional boundary for conductance through the set correction angle.

Figure 204 - Conductance protection operation characteristic



Conductance: Forward Conductance: Reverse Conductance: Non-directional

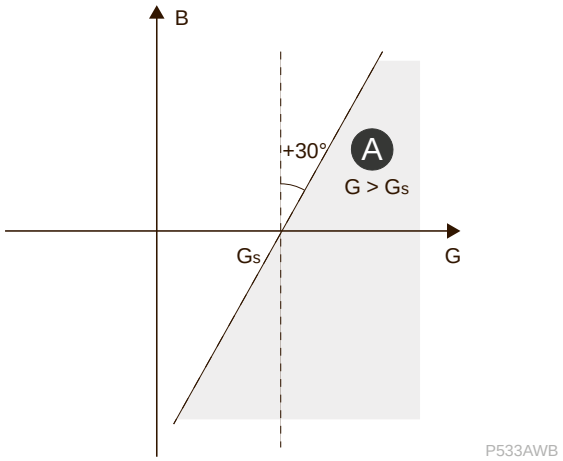
A Operate zone

NOTE:

Center of the characteristic area for forward direction occurs when IN is in phase with -VN.

Assuming that the direction of the G axis is 0°. If the correction angle is set to +30°, this rotates the boundary from 90°...270° to 60°...240°.

Figure 205 - Conductance protection operation characteristic with +30° correction angle

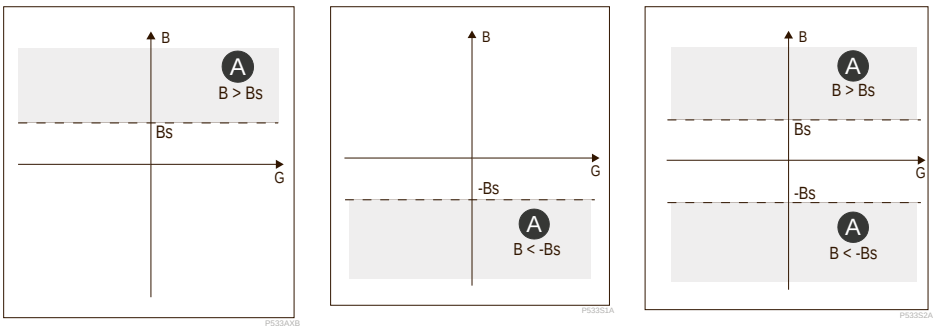


A Operate zone

Operation of susceptance protection

The susceptance protection may be set to non-directional, forward or reverse. Hence, provided the magnitude and the directional criteria are met for susceptance, the PowerLogic P5 protection relay will operate. The correction angle causes rotation of the directional boundary for susceptance through the set correction angle.

Figure 206 - Susceptance protection operation characteristic



Susceptance: Forward Susceptance: Reverse Susceptance: Non-directional

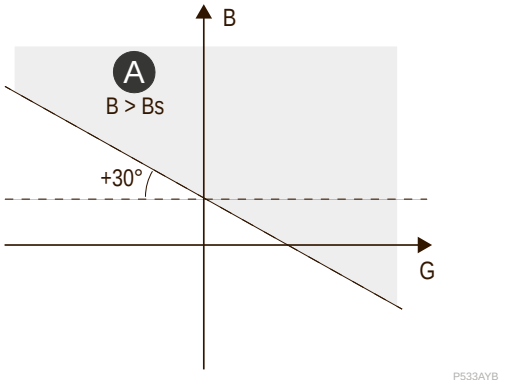
A Operate zone

NOTE:

Center of characteristic area for forward direction occurs when IN leads -VN by 90°.

Assuming that the direction of the G axis indicates 0°. If the correction angle is set to +30°, this rotates the boundary from 0°...180° to 330°...150°.

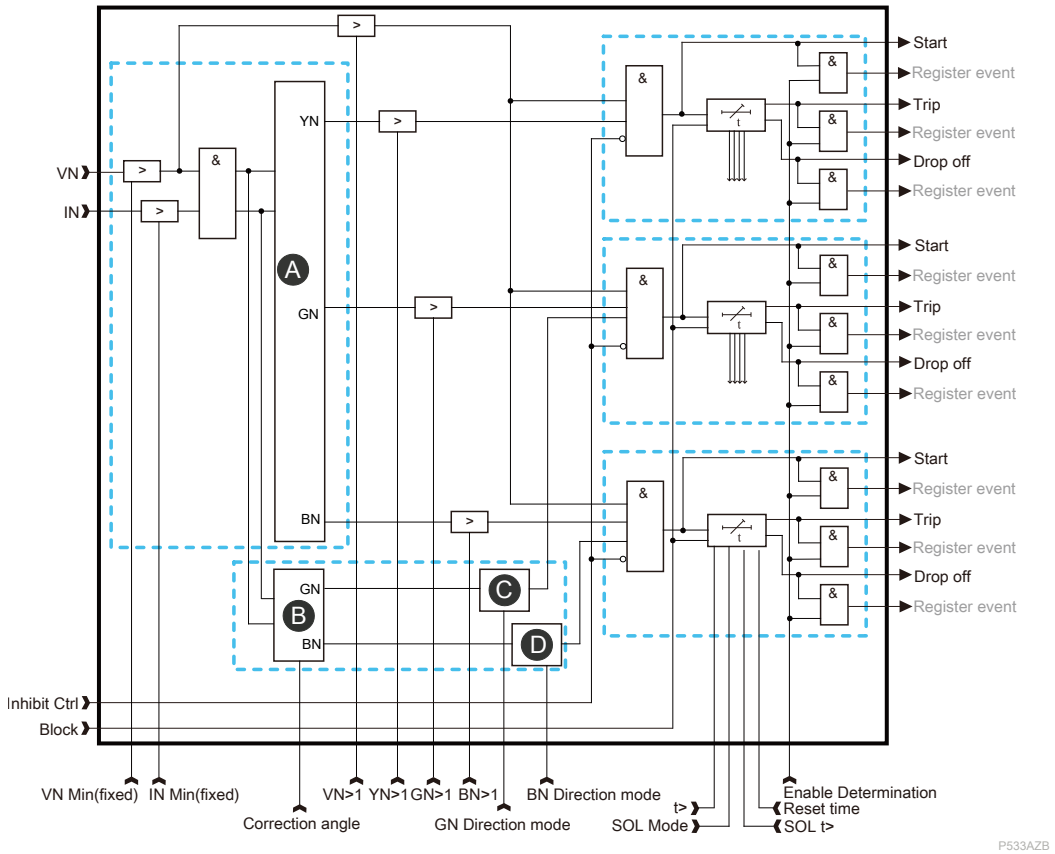
Figure 207 - Susceptance protection operation characteristic with +30° correction angle



A	Operate zone

Block diagram

Figure 208 - Block diagram of the neutral admittance protection



A	Admittance Calculation	B	Direction Determination
C	GN Mode = Non dir or GN Mode = GN dir	D	BN Mode = Non dir or BN Mode = BN dir

Characteristics

Table 59 - Settings and characteristics of the neutral admittance protection

Settings/ characteristics (description/label)	Values
Enable All YN>/All YN>[56]	
Options	Off/On
VN pick-up value/VN>	
Setting range	0.005...0.800 pu[57] for measured values 0.020...0.800 pu[57] for calculated values
Resolution	0.001
Accuracy	±5%
Reset ratio	95% ± 2%
VN minimum	
Value	0.004 pu[57] (fixed) for measured values 0.019 pu[57] (fixed) for calculated values
IN minimum	
Value	0.1 A primary (fixed), for current measured by CSH core balance CT (2A) 1 A primary (fixed), for current measured by CSH core balance CT (20A) 0.005 pu[58] (fixed) for current measured by sensitive EF CT 0.02 pu[58] (fixed) for current measured by standard EF CT 0.005 pu[58] (fixed) for current measured by standard EF CT (for CSH30 use) 0.05 pu[58] (fixed) for calculated EF current value
Enable YN>1/GN>1/BN>1[59]	
Options	Off/On
Pick-up value/YN>1	
Setting range	(1%...200%) IN/VN[60] for current measured by sensitive earth/ground fault CTs (5%...1000%) IN/VN[60] for current measured by standard earth/ground fault CTs (5%...1000%) IN/VN[60] for current measured by standard earth/ground fault CTs (for CSH30 use) (25%...5000%) IN/VN[60] for current measured by 2A CSH, 20A CSH, and for current value that is calculated
Resolution	1% IN/VN[60] for current measured by sensitive earth/ground fault CTs 5% IN/VN[60] for current measured by standard earth/ground fault CTs 25% IN/VN[60] for current measured by 2A CSH, 20A CSH, and for current value that is calculated
Accuracy	±5%
Reset ratio	90% ± 5%
Pick-up value/GN>1	
Setting range	(1%...100%) IN/VN[60] for current measured by sensitive earth/ground fault CTs (5%...500%) IN/VN[60] for current measured by standard earth/ground fault CTs (5%...500%) IN/VN[60] for current measured by standard earth/ground fault CTs (for CSH30 use) (25%...2500%) IN/VN[60] for current measured by 2A CSH, 20A CSH, and for current value that is calculated
Resolution	1% IN/VN[60] for current measured by sensitive earth/ground fault CTs 5% IN/VN[60] for current measured by standard earth/ground fault CTs 25% IN/VN[60] for current measured by 2A CSH, 20A CSH, and for current value that is calculated

56. General protection stage on/off control
57. Vnom = VT primary nominal (PP)
58. Inom
59. This setting does not take effect if the general protection stage control is set to Off. See the previous footnote.
60. YN.nom