Relion® 650 SERIES

650 series
Version 1.3 IEC
Cyber security deployment guideline
Copyright

This document and parts thereof must not be reproduced or copied without written permission from ABB, and the contents thereof must not be imparted to a third party, nor used for any unauthorized purpose.

The software and hardware described in this document is furnished under a license and may be used or disclosed only in accordance with the terms of such license.

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org/)

This product includes cryptographic software written/developed by: Eric Young (eay@cryptsoft.com) and Tim Hudson (tjh@cryptsoft.com).

Trademarks

ABB and Relion are registered trademarks of the ABB Group. All other brand or product names mentioned in this document may be trademarks or registered trademarks of their respective holders.

Warranty

Please inquire about the terms of warranty from your nearest ABB representative.

ABB AB
Grid Automation Products
SE-721 59 Västerås
Sweden
Telephone: +46 (0) 21 32 50 00
Facsimile: +46 (0) 21 14 69 18
http://www.abb.com/protection-control
Disclaimer

The data, examples and diagrams in this manual are included solely for the concept or product description and are not to be deemed as a statement of guaranteed properties. All persons responsible for applying the equipment addressed in this manual must satisfy themselves that each intended application is suitable and acceptable, including that any applicable safety or other operational requirements are complied with. In particular, any risks in applications where a system failure and/or product failure would create a risk for harm to property or persons (including but not limited to personal injuries or death) shall be the sole responsibility of the person or entity applying the equipment, and those so responsible are hereby requested to ensure that all measures are taken to exclude or mitigate such risks.

This document has been carefully checked by ABB but deviations cannot be completely ruled out. In case any errors are detected, the reader is kindly requested to notify the manufacturer. Other than under explicit contractual commitments, in no event shall ABB be responsible or liable for any loss or damage resulting from the use of this manual or the application of the equipment.
Conformity

This product complies with the directive of the Council of the European Communities on the approximation of the laws of the Member States relating to electromagnetic compatibility (EMC Directive 2004/108/EC) and concerning electrical equipment for use within specified voltage limits (Low-voltage directive 2006/95/EC). This conformity is the result of tests conducted by ABB in accordance with the product standards EN 50263 and EN 60255-26 for the EMC directive, and with the product standards EN 60255-1 and EN 60255-27 for the low voltage directive. The product is designed in accordance with the international standards of the IEC 60255 series.
# Table of contents

## Section 1 Introduction

1.1 This manual.................................................................................................... 3  
1.2 Document revision history.......................................................................... 3  
1.3 Related documents....................................................................................... 3  

## Section 2 Security in Substation Automation

2.1 General security in Substation Automation............................................ 5  

## Section 3 Secure system setup

3.1 Physical interfaces....................................................................................... 7  
3.2 IP ports......................................................................................................... 7  
3.3 FTP access with SSL FTPACCS................................................................. 9  
3.4 Encryption algorithms............................................................................... 9  
3.5 Denial of service......................................................................................... 10  
3.6 Certificate handling.................................................................................. 10  

## Section 4 Managing user roles and user accounts

4.1 Authorization............................................................................................. 11  
4.2 Predefined user roles............................................................................... 12  
4.3 Password policies..................................................................................... 14  
4.4 IED User management............................................................................. 14  
4.4.1 Starting IED user management............................................................ 15  
4.4.2 General settings................................................................................ 15  
4.4.3 User profile management................................................................. 16  
4.4.3.1 Adding new users........................................................................ 17  
4.4.3.2 Adding users to new user roles..................................................... 19  
4.4.3.3 Deleting existing users............................................................... 20  
4.4.3.4 Changing password..................................................................... 22  
4.4.4 User role management....................................................................... 23  
4.4.4.1 Adding new users to user roles.................................................... 23  
4.4.4.2 Deleting existing User from user roles....................................... 24  
4.4.4.3 Reusing user accounts................................................................. 24  
4.4.5 Writing user management settings to the IED................................. 25  
4.4.6 Reading user management settings from the IED........................... 25  
4.4.7 Saving user management settings.................................................... 25  

## Section 5 User activity logging

5.1 Activity logging ACTIVLOG...................................................................... 27  
5.2 Generic security application AGSAL..................................................... 28  
5.3 Security alarm SECALARM................................................................. 28  
5.4 About Security events.......................................................................... 29  
5.5 Event types......................................................................................... 29  

© Copyright 2013 ABB. All rights reserved
<table>
<thead>
<tr>
<th>Section 6</th>
<th>Local HMI use........................................................................................................... 33</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>Logging on.................................................................................................................... 33</td>
</tr>
<tr>
<td>6.2</td>
<td>Logging off................................................................................................................. 35</td>
</tr>
<tr>
<td>6.3</td>
<td>Saving settings.......................................................................................................... 36</td>
</tr>
<tr>
<td>6.4</td>
<td>Recovering password................................................................................................. 37</td>
</tr>
<tr>
<td>Section 7</td>
<td>IEEE Compliance statement....................................................................................... 41</td>
</tr>
<tr>
<td>7.1</td>
<td>IEEE1686 compliance.................................................................................................. 41</td>
</tr>
<tr>
<td>Section 8</td>
<td>Glossary...................................................................................................................... 45</td>
</tr>
</tbody>
</table>
Section 1  Introduction

1.1  This manual

Cyber Security Deployment Guidelines describes password procedures and levels of access in the system.

1.2  Document revision history

<table>
<thead>
<tr>
<th>Document revision/date</th>
<th>History</th>
</tr>
</thead>
<tbody>
<tr>
<td>-/March 2013</td>
<td>First release</td>
</tr>
<tr>
<td>A/October 2016</td>
<td>Minor corrections made</td>
</tr>
<tr>
<td>B/November 2019</td>
<td>Maintenance release - Updated safety information and bug corrections</td>
</tr>
</tbody>
</table>

1.3  Related documents

Documents related to REB650

<table>
<thead>
<tr>
<th>Identity number</th>
</tr>
</thead>
<tbody>
<tr>
<td>1MRK 505 287-UEN</td>
</tr>
</tbody>
</table>

Documents related to REL650

<table>
<thead>
<tr>
<th>Identity number</th>
</tr>
</thead>
<tbody>
<tr>
<td>1MRK 506 334-UEN</td>
</tr>
</tbody>
</table>

Documents related to RET650

<table>
<thead>
<tr>
<th>Identity number</th>
</tr>
</thead>
<tbody>
<tr>
<td>1MRK 504 134-UEN</td>
</tr>
</tbody>
</table>

Documents related to REC650

<table>
<thead>
<tr>
<th>Identity number</th>
</tr>
</thead>
<tbody>
<tr>
<td>1MRK 511 286-UEN</td>
</tr>
</tbody>
</table>

Table continues on next page
<table>
<thead>
<tr>
<th>Documents related to REC650</th>
<th>Identity number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Product Guide</td>
<td>1MRK 511 289-BEN</td>
</tr>
<tr>
<td>Type test certificate</td>
<td>1MRK 511 289-TEN</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Documents related to REG650</th>
<th>Identity number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application manual</td>
<td>1MRK 502 047-UEN</td>
</tr>
<tr>
<td>Technical manual</td>
<td>1MRK 502 048-UEN</td>
</tr>
<tr>
<td>Commissioning manual</td>
<td>1MRK 502 049-UEN</td>
</tr>
<tr>
<td>Product Guide</td>
<td>1MRK 502 050-BEN</td>
</tr>
<tr>
<td>Type test certificate</td>
<td>1MRK 502 050-TEN</td>
</tr>
<tr>
<td>Rotor Earth Fault Protection with Injection Unit RXTTE4 and REG670</td>
<td>1MRG001910</td>
</tr>
<tr>
<td>Application notes for Circuit Breaker Control</td>
<td>1MRG006806</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Documents related to REQ650</th>
<th>Identity number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application manual</td>
<td>1MRK 505 291-UEN</td>
</tr>
<tr>
<td>Technical manual</td>
<td>1MRK 505 292-UEN</td>
</tr>
<tr>
<td>Commissioning manual</td>
<td>1MRK 505 293-UEN</td>
</tr>
<tr>
<td>Product Guide</td>
<td>1MRK 505 294-BEN</td>
</tr>
<tr>
<td>Type test certificate</td>
<td>1MRK 505 294-TEN</td>
</tr>
<tr>
<td>Application notes for Circuit Breaker Control</td>
<td>1MRG006806</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>650 series manuals</th>
<th>Identity number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Communication protocol manual, DNP 3.0</td>
<td>1MRK 511 280-UEN</td>
</tr>
<tr>
<td>Communication protocol manual, IEC 61850–8–1</td>
<td>1MRK 511 281-UEN</td>
</tr>
<tr>
<td>Communication protocol manual, IEC 60870-5-103</td>
<td>1MRK 511 282-UEN</td>
</tr>
<tr>
<td>Cyber Security deployment guidelines</td>
<td>1MRK 511 285-UEN</td>
</tr>
<tr>
<td>Point list manual, DNP 3.0</td>
<td>1MRK 511 283-UEN</td>
</tr>
<tr>
<td>Engineering manual</td>
<td>1MRK 511 284-UEN</td>
</tr>
<tr>
<td>Operation manual</td>
<td>1MRK 500 096-UEN</td>
</tr>
<tr>
<td>Installation manual</td>
<td>1MRK 514 016-UEN</td>
</tr>
<tr>
<td>Accessories, 650 series</td>
<td>1MRK 513 023-BEN</td>
</tr>
<tr>
<td>MICS</td>
<td>1MRG 010 656</td>
</tr>
<tr>
<td>PICS</td>
<td>1MRG 010 660</td>
</tr>
<tr>
<td>PIXIT</td>
<td>1MRG 010 658</td>
</tr>
</tbody>
</table>
Section 2 Security in Substation Automation

2.1 General security in Substation Automation

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

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

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

ABB fully understands the importance of cyber security and its role in advancing the security of substation automation systems. A customer investing in new ABB technologies can rely on system solutions where reliability and security have the highest priority.

Figure 1: System architecture for substation automation system
Section 3 Secure system setup

3.1 Physical interfaces

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

3.2 IP ports

The IP port security guideline cannot suggest concrete products for a secure system setup. This must be decided within the specific project, requirements and existing infrastructure. The required external equipment can be separate devices or devices that combine firewall, router and secure VPN functionality.

To set up an IP firewall the following table summarizes the IP ports used in the 650 series. The ports are listed in ascending order. The column “Default state” defines whether a port is open or closed by default. All ports that are closed can be opened as described in the comment column in the table. Front and Rear refer to the physical front and rear port. The protocol availability on these ports is configurable.

ABB recommends using common security measures, like firewalls, up to date anti virus software, etc. to protect the IED and the equipment around it.

<table>
<thead>
<tr>
<th>Port</th>
<th>Protocol</th>
<th>Default state</th>
<th>Front</th>
<th>Rear</th>
<th>Service</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>21</td>
<td>TCP</td>
<td>Open</td>
<td>OFF</td>
<td>OFF</td>
<td>FTP</td>
<td>File transfer protocol</td>
</tr>
<tr>
<td>67</td>
<td>UDP</td>
<td>Open</td>
<td>ON</td>
<td>N/A</td>
<td>DHCP</td>
<td>Front port only, RJ45</td>
</tr>
<tr>
<td>102</td>
<td>TCP</td>
<td>Open</td>
<td>OFF</td>
<td>ON</td>
<td>IEC 61850</td>
<td>MMS communication</td>
</tr>
<tr>
<td>123</td>
<td>UDP</td>
<td>Closed</td>
<td>OFF</td>
<td>OFF</td>
<td>SNTP</td>
<td>Enabled when IED is configured as SNTP master. 1)</td>
</tr>
<tr>
<td>990</td>
<td>UDP</td>
<td>Open</td>
<td>ON</td>
<td>OFF</td>
<td>FTPS</td>
<td>FTP with implicit SSL</td>
</tr>
<tr>
<td>7001</td>
<td>TCP</td>
<td>Closed</td>
<td>OFF</td>
<td>OFF</td>
<td>FST</td>
<td>SPA protocol on TCP/IP used by FST (Field Service Tool)</td>
</tr>
<tr>
<td>2102</td>
<td>TCP</td>
<td>Open</td>
<td>ON</td>
<td>ON</td>
<td>PCM Access (IED configuration protocol)</td>
<td>IED configuration protocol</td>
</tr>
<tr>
<td>20000</td>
<td>TCP</td>
<td>Closed</td>
<td>OFF</td>
<td>ON</td>
<td>DNP3</td>
<td>DNP3.0 DNP communication only</td>
</tr>
<tr>
<td>20000</td>
<td>UDP</td>
<td>Closed</td>
<td>OFF</td>
<td>ON</td>
<td>DNP3</td>
<td>DNP3.0 DNP communication only</td>
</tr>
<tr>
<td>49220-49235</td>
<td>TCP</td>
<td>Closed</td>
<td>ON</td>
<td>ON</td>
<td>FTP</td>
<td>TCP data ports for FTP PASV command. Ports open on demand.</td>
</tr>
</tbody>
</table>

1) When the IED is configured as a SNTP client it will use the first ephemeral port available. The range of ephemeral ports is 1024 to 5000.

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

See the 650 series technical manual and the corresponding protocol documentation on how to configure a certain communication protocol for the 650 series.

There are some restrictions and dependencies:

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

If the FTP port is changed PCM600 cannot be used since it is not possible to configure it to use other IP-ports than port 21 for FTP.

PCM600 uses IED configuration protocol (TCP port 2102) and FTP ports to communicate with the IED. The port used by the IED configuration protocol is fixed and cannot be changed. FTP port is used for uploading disturbance records (DR).

For Field service tool, the IP port for a proprietary SPA protocol is used (TCP port 7001) and the port is fixed and cannot be changed.

IP routing is not possible via any of the physical interfaces.

Some IP ports are not possible to use in all physical interfaces.

![Figure 2: Ethernet port used for PCM600 only, front view](image)
3.3 FTP access with SSL FTPACCS

The FTP Client defaults to the best possible security mode when trying to negotiate with SSL.

The automatic negotiation mode acts on port number and server features. It tries to immediately activate implicit SSL if the specified port is 990. If the specified port is any other, it tries to negotiate with explicit SSL via AUTH SSL/TLS.

Using FTP without SSL encryption gives the FTP client reduced capabilities. This mode is only for accessing disturbance recorder data from the IED.

If normal FTP is required to read out disturbance recordings, create a specific account for this purpose with rights only to do File transfer. The password of this user will be exposed in clear text on the wire.

3.4 Encryption algorithms

SSL/TLS connections are encrypted with AES 256 if possible or AES 128 as a minimum. At startup a negotiation decides between these two options.

No passwords are stored in clear text within the IED. A hashed representation of the passwords with SHA 256 is stored in the IED. These are not accessible from outside via any ports.

IED supports TLS versions up to 1.2 (1.0, 1.1 and 1.2), decided by the client.
3.5 Denial of service

The denial of service function is designed to limit the CPU load that can be produced by the Ethernet network traffic on the IED. The communication facilities must not be allowed to compromise the primary functionality of the device. All inbound network traffic is quota controlled, so that a too heavy network load can be controlled. Heavy network load might for instance be the result of malfunctioning equipment connected to the network.

The denial of service functions DOSFRNT, DOSLAN1 measure the IED load from communication and, if necessary, limits it from jeopardizing the IED’s control and protection functionality due to a high CPU load. The function has the following outputs:

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

For more information see related documents.

3.6 Certificate handling

A self-signed certificate is signed by the IED it certifies. Certificates use encryption to provide secure communication over the network. Certificate encryption strength depends on the certificate authority (CA).

The certificate is always trusted during communication between the IED and PCM600.

If Windows is configured to use UAC High the certificate have to be manually trusted in a dialog box.
Section 4  Managing user roles and user accounts

4.1  Authorization

The user roles with different user rights are predefined in the IED.

The IED users can be created, deleted and edited only with PCM600. One user can belong to one or several user roles.

At delivery, the IED user has full access as SuperUser until users are created with PCM600.

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

Table 2: Default users

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

Changes in user management settings do not cause an IED reboot.

After three consecutive failed login attempts the user will be locked out for ten minutes before a new attempt to log in can be performed. This time is settable 10 minutes to 60 minutes.
The PCM600 tool caches the login credentials after successful login for 15 minutes. During that time no more login will be necessary.

4.2 Predefined user roles

There are different roles of users that can access or operate different areas of the IED and tool functionalities.

Ensure that the user logged on to the IED has the required access when writing particular data to the IED from PCM600. For more information about setting user access rights, see the PCM600 documentation.

The meaning of the legends used in the table:

- **X** = Full access rights
- **R** = Only reading rights
- **-** = No access rights

<table>
<thead>
<tr>
<th>Access rights</th>
<th>VIEWER</th>
<th>OPERATOR</th>
<th>ENGINEER</th>
<th>INSTALLER</th>
<th>SECADM</th>
<th>SECAUD</th>
<th>RBACMNT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Config – Basic</td>
<td>-</td>
<td>-</td>
<td>X</td>
<td>X</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Config – Advanced</td>
<td>-</td>
<td>-</td>
<td>X</td>
<td>X</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>FileTransfer – Tools</td>
<td>-</td>
<td>-</td>
<td>X</td>
<td>X</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>UserAdministration</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>X</td>
<td>-</td>
<td>X</td>
</tr>
<tr>
<td>Setting – Basic</td>
<td>R</td>
<td>-</td>
<td>X</td>
<td>X</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Setting – Advanced</td>
<td>R</td>
<td>-</td>
<td>X</td>
<td>X</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Control – Basic</td>
<td>-</td>
<td>X</td>
<td>X</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Control – Advanced</td>
<td>-</td>
<td>X</td>
<td>X</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>IEDCmd – Basic</td>
<td>-</td>
<td>X</td>
<td>X</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>IEDCmd – Advanced</td>
<td>-</td>
<td>-</td>
<td>X</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>FileTransfer – Limited</td>
<td>-</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>DB Access normal</td>
<td>-</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Audit log read</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>X</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Setting – Change Setting Group</td>
<td>-</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Security Advanced</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>X</td>
<td>-</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Access rights</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Config – Basic</td>
<td>Configuration – Basic is intended for engineers that only adapt an existing configuration e.g. the I/O-Configuration using SMT</td>
</tr>
<tr>
<td>Config – Advanced</td>
<td>Configuration – Advanced is intended for engineers that do the whole application engineering and using e.g. ACT</td>
</tr>
<tr>
<td>FileTransfer – Tools</td>
<td>FileTransfer – Tools is used for some configuration files for the configuration and shall have the same value as Config – Advanced</td>
</tr>
<tr>
<td>UserAdministration</td>
<td>UserAdministration is used to handle user management e.g. adding new user</td>
</tr>
</tbody>
</table>

Table continues on next page
<table>
<thead>
<tr>
<th>Access rights</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Setting – Basic</td>
<td>Setting – Basic is used for basic settings e.g. control settings and limit supervision</td>
</tr>
<tr>
<td>Setting – Advanced</td>
<td>Setting – Advanced is used for the relay engineer to set settings e.g. for the protection functions</td>
</tr>
<tr>
<td>Control – Basic</td>
<td>Control – Basic is used for a normal operator without possibility to bypass safety functions e.g. interlock or synchro-check bypass</td>
</tr>
<tr>
<td>Control – Advanced</td>
<td>Control – Advanced is used for an operator that is trusted to do process commands that can be dangerous</td>
</tr>
<tr>
<td>IEDCmd – Basic</td>
<td>IEDCmd – Basic is used for commands to the IED that are not critical e.g. Clear LEDs, manual triggering of disturbances</td>
</tr>
<tr>
<td>IEDCmd – Advanced</td>
<td>IEDCmd – Advanced is used for commands to the IED that can hide information e.g. Clear disturbance record</td>
</tr>
<tr>
<td>FileTransfer – Limited</td>
<td>FileTransfer - Limited is used for access to disturbance files e.g. through FTP</td>
</tr>
<tr>
<td>DB Access normal</td>
<td>Database access for normal user. This is needed for all users that access data from PCM</td>
</tr>
<tr>
<td>Audit log read</td>
<td>Audit log read allows reading the audit log from the IED</td>
</tr>
<tr>
<td>Setting – Change Setting Group</td>
<td>Setting – Change Setting Group is separated to be able to include the possibility to change the setting group without changing any other setting</td>
</tr>
<tr>
<td>Security Advanced</td>
<td>Security Advanced is the privilege required to do some of the more advanced security-related settings</td>
</tr>
</tbody>
</table>

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

At delivery, the IED has a default user defined with full access rights. PCM600 uses this default user to access the IED. This user is automatically removed in IED when users are defined via the IED Users tool in PCM600.

Default User ID: Administrator

Password: Administrator

Only characters A - Z, a - z and 0 - 9 shall be used in user names. User names are not case sensitive. For passwords see the Password policies in PCM600.

First user created must be appointed the role SECADM to be able to write users, created in PCM600, to the IED.

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

Do not use access rights “FileLoading”, “FileDumping”, “File Transfer (Super)”, and “DB Access super” in PCM600.
4.3 Password policies

Only ASCII characters are allowed when typing username or password. Currently passwords in the range 32-126 and 192-383 (ASCII ranges, decimal) are supported.

Password policies are set in the IED Users tool in PCM600. There are several options for forcing the password safer.

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

To achieve IEEE 1686 conformity, a password with a minimum length of 8 characters must be used, and the square Enforce Password Policies shall be ticked.

Settings for password lifetime are not supported in this release.

4.4 IED User management

The IED Users tool in PCM600 is used for editing user profiles and role assignments.

In the IED Users tool, the data can be retrieved from an IED or data can be written to an IED if permitted. The data from an IED can be saved to the project database.
Always use Read User Management Settings from IED before making any changes when managing user profiles. If this is not done, password changes made by users may be lost!

Nothing is changed in the IED until a “writing-to-IED operation” is performed.

### 4.4.1 Starting IED user management

- Connect the PC to the IED
- Start PCM600
- Select an IED in the object tree
- Select Tools/IED Users or,
- Right-click an IED in the object tree and select IED Users
  The IED User dialog box appears.

### 4.4.2 General settings

In the General tab, by clicking Restore factory settings the default users can be restored in the IED Users tool. For the 650 series, this means reverting back to the factory delivered users. Performing this operation does not remove the users in the IED. Nothing is changed in the IED until a “writing-to-IED operation” is performed.

This is not the same action as Revert to IED defaults in the recovery menu.

The previous administrator user ID and password have to be given so that the writing toward the IED can be done.

Editing can be continued by clicking on Restore factory settings when not connected to the IED.
4.4.3 User profile management

In the User Management tab, the user profiles of the selected IED can be edited. New users can be created, existing users can be deleted and different user group members can be edited.

A user profile must always belong to at least one user group.
4.4.3.1 Adding new users

1. Click in the Users tab to open the wizard.
Section 4
Managing user roles and user accounts

Figure 8: Create new user

2. Follow the instructions in the wizard to define a user name, password and user group. Select at least one user group where the defined user belongs. The user profile can be seen in the User details field.

Figure 9: Select user groups

3. Select the user from the user list and type a new name or description in the Description/full name field to change the name or description of the user.
4.4.3.2 Adding users to new user roles

1. Select the user from the Users list.
2. Select the new role from the Select a role list.
3. Click.

Information about the roles to which the user belongs to can be seen in the User details area.
Section 4
Managing user roles and user accounts

Figure 11: Adding user

4.4.3.3 Deleting existing users

1. Select the user from the Users list.
2. Click.

**Figure 12:** Select user to be deleted

**Figure 13:** Delete existing user
4.4.3.4 Changing password

1. Select the user from the Users list.

![RTL550 - IED Users](image)

*Figure 14: Select user*

2. Click 🌐.

3. Type the old password once and the new password twice in the required fields. The passwords can be saved in the project database or sent directly to the IED.

No passwords are stored in clear text within the IED. A hash representation of the passwords is stored in the IED and it is not accessible from outside via any ports.
4.4.4 User role management

In the Roles tab, the user roles can be modified. The user's memberships to specific roles can be modified with a list of available user roles and users.

4.4.4.1 Adding new users to user roles

1. Select the required role from the Roles list.
The role profile can be seen under the Role details field.

2. Select the new user from the Select a user list.
3. Click +.
   The new user is shown in the Users assigned list.

### 4.4.4.2 Deleting existing User from user roles

1. Right-click the user in the Users assigned list.
2. Select Remove this Role from Selected Member.

![Figure 17: Remove Role from User](image)

### 4.4.4.3 Reusing user accounts

IED user account data can be exported from one IED and imported to another. The data is stored in an encrypted file.

To export IED user account data from an IED

1. Click the Import Export tab in the IED User tool in PCM600.
2. Click Export IED account data.

   The user account data is exported to a file with user defined filename and location.

Import IED user rights to an IED

1. Click Import IED account data.
2. Open the previously exported file.
Only users who have the right to change the user account data in PCM600 are allowed to export and import.

![R650 - IED Users](image)

**Figure 18: Importing and exporting user account data**

### 4.4.5 Writing user management settings to the IED

- Click the **Write User Management Settings to IED** button on the toolbar.

![Local Server Test - PCM600](image)

**Figure 19: Write to IED**

The data is saved when writing to the IED starts.

### 4.4.6 Reading user management settings from the IED

- Click the **Read User Management Settings from IED** button on the toolbar.

### 4.4.7 Saving user management settings

- Select **File/Save** from the menu.
- Click the **Save** toolbar button.

The save function is enabled only if the data has changed.
Section 5  User activity logging

5.1 Activity logging ACTIVLOG

ACTIVLOG contains all settings for activity logging.

There can be 6 external log servers to send syslog events to. Each server can be configured with IP address; IP port number and protocol format. The format can be either syslog (RFC 5424) or Common Event Format (CEF) from ArcSight.

<table>
<thead>
<tr>
<th>Name</th>
<th>Values (Range)</th>
<th>Unit</th>
<th>Step</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ExtLogSrv1Type</td>
<td>Off SYSLOG UDP/IP</td>
<td></td>
<td></td>
<td>Off</td>
<td>External log server 1 type</td>
</tr>
<tr>
<td>ExtLogSrv1Port</td>
<td>1 - 65535</td>
<td></td>
<td>1</td>
<td>514</td>
<td>External log server 1 port number</td>
</tr>
<tr>
<td>ExtLogSrv1IP</td>
<td>IP Address 1</td>
<td></td>
<td>1</td>
<td>127.0.0.1</td>
<td>External log server 1 IP-address</td>
</tr>
<tr>
<td>ExtLogSrv2Type</td>
<td>Off SYSLOG UDP/IP</td>
<td></td>
<td></td>
<td>Off</td>
<td>External log server 2 type</td>
</tr>
<tr>
<td>ExtLogSrv2Port</td>
<td>1 - 65535</td>
<td></td>
<td>1</td>
<td>514</td>
<td>External log server 2 port number</td>
</tr>
<tr>
<td>ExtLogSrv2IP</td>
<td>IP Address 1</td>
<td></td>
<td>1</td>
<td>127.0.0.1</td>
<td>External log server 2 IP-address</td>
</tr>
<tr>
<td>ExtLogSrv3Type</td>
<td>Off SYSLOG UDP/IP</td>
<td></td>
<td></td>
<td>Off</td>
<td>External log server 3 type</td>
</tr>
<tr>
<td>ExtLogSrv3Port</td>
<td>1 - 65535</td>
<td></td>
<td>1</td>
<td>514</td>
<td>External log server 3 port number</td>
</tr>
<tr>
<td>ExtLogSrv3IP</td>
<td>IP Address 1</td>
<td></td>
<td>1</td>
<td>127.0.0.1</td>
<td>External log server 3 IP-address</td>
</tr>
<tr>
<td>ExtLogSrv4Type</td>
<td>Off SYSLOG UDP/IP</td>
<td></td>
<td></td>
<td>Off</td>
<td>External log server 4 type</td>
</tr>
<tr>
<td>ExtLogSrv4Port</td>
<td>1 - 65535</td>
<td></td>
<td>1</td>
<td>514</td>
<td>External log server 4 port number</td>
</tr>
<tr>
<td>ExtLogSrv4IP</td>
<td>IP Address 1</td>
<td></td>
<td>1</td>
<td>127.0.0.1</td>
<td>External log server 4 IP-address</td>
</tr>
<tr>
<td>ExtLogSrv5Type</td>
<td>Off SYSLOG UDP/IP</td>
<td></td>
<td></td>
<td>Off</td>
<td>External log server 5 type</td>
</tr>
<tr>
<td>ExtLogSrv5Port</td>
<td>1 - 65535</td>
<td></td>
<td>1</td>
<td>514</td>
<td>External log server 5 port number</td>
</tr>
<tr>
<td>ExtLogSrv5IP</td>
<td>IP Address 1</td>
<td></td>
<td>1</td>
<td>127.0.0.1</td>
<td>External log server 5 IP-address</td>
</tr>
</tbody>
</table>

Table continues on next page
### Generic security application AGSAL

As a logical node AGSAL is used for monitoring security violation regarding authorization, access control and inactive association including authorization failure. Therefore, all the information in AGSAL can be configured to report to 61850 client.

#### Security alarm SECALARM

The function creates and distributes security events for mapping the security events on protocols such as DNP3.

It is possible to map respective protocol to the signals of interest and configure them for monitoring with the Communication Management tool (CMT) in PCM600. No events are mapped by default.

Parameter names:
- EVENTID: Event ID of the generated security event
- SEQNUMBER: Sequence number of the generated security event

![SECALARM](IEC13000006-v1-en vsd)

**Figure 20: Function block, Security alarm SECALARM**

### Table 7: SECALARM Non group settings (basic)

<table>
<thead>
<tr>
<th>Name</th>
<th>Values (Range)</th>
<th>Unit</th>
<th>Step</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operation</td>
<td>Off On</td>
<td></td>
<td></td>
<td>On</td>
<td>Operation On/Off</td>
</tr>
</tbody>
</table>

### Table 8: SECALARM Output signals

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>EVENTID</td>
<td>INTEGER</td>
<td>Eventid of the generated security event</td>
</tr>
<tr>
<td>SEQNUMBER</td>
<td>INTEGER</td>
<td>Sequence number of the generated security event</td>
</tr>
</tbody>
</table>
5.4 About Security events

Relevant user operations are logged as security events. A security event contains an event ID, a
time stamp, a sequence number, the user name, the severity of the action and the name of the
source. These events can be sent to external security log servers using Syslog. The log servers
are configured from PCM600. Syslog is a standard protocol for event logging.

To be able to access the security logs the user need the role SECAUD (security
auditor) or the access right “Audit log read”.

5.5 Event types

All user activities are logged and stored according to IEC 61850.

Table 9: Event type codes

<table>
<thead>
<tr>
<th>Event number</th>
<th>Acronyms</th>
<th>GSAL mapping</th>
<th>English</th>
</tr>
</thead>
<tbody>
<tr>
<td>1110</td>
<td>LOGIN_OK</td>
<td>GSAL.Ina</td>
<td>Login successful</td>
</tr>
<tr>
<td>1130</td>
<td>LOGIN_FAIL_WRONG_CR</td>
<td>GSAL.AuthFail</td>
<td>Login failed - Wrong credentials</td>
</tr>
<tr>
<td>1170</td>
<td>LOGIN_FAIL_3_TIMES</td>
<td>GSAL.AuthFail</td>
<td>Login failed 3 times</td>
</tr>
<tr>
<td>1210</td>
<td>LOGOUT_USER</td>
<td>GSAL.Ina</td>
<td>Logout (user logged out)</td>
</tr>
<tr>
<td>1220</td>
<td>LOGOUT_TIMEOUT</td>
<td>GSAL.Ina</td>
<td>Logout by user inactivity (timeout)</td>
</tr>
<tr>
<td>1460</td>
<td>PARAM_CHANGE_FAIL_RIGHTS</td>
<td>GSAL.AcsCtlFail</td>
<td>Parameter changes failed — no rights</td>
</tr>
<tr>
<td>1710</td>
<td>CONFIG_RESET_FACTORY_DEF</td>
<td>GSAL.Ina</td>
<td>Device reset to factory default</td>
</tr>
<tr>
<td>2110</td>
<td>USER_ACCNT_CREATE_OK</td>
<td>GSAL.Ina</td>
<td>User account created successfully</td>
</tr>
<tr>
<td>2120</td>
<td>USER_ACCNT_DEL_OK</td>
<td>GSAL.Ina</td>
<td>User account deleted successfully</td>
</tr>
<tr>
<td>2130</td>
<td>USER_ACCNT_CREATE_FAIL</td>
<td>GSAL.SvcViol</td>
<td>User account creation failed</td>
</tr>
<tr>
<td>2140</td>
<td>USER_ACCNT_DEL_FAIL</td>
<td>GSAL.SvcViol</td>
<td>User account deletion failed</td>
</tr>
<tr>
<td>2160</td>
<td>USER_NEW_ROLE_OK</td>
<td>GSAL.Ina</td>
<td>New role assigned to user successfully</td>
</tr>
<tr>
<td>2170</td>
<td>USER_ROLE_REMOVED_OK</td>
<td>GSAL.SvcViol</td>
<td>User role assignment removed successfully</td>
</tr>
<tr>
<td>2210</td>
<td>USER_PW_CHANGE_OK</td>
<td>GSAL.SvcViol</td>
<td>User password changed successfully</td>
</tr>
<tr>
<td>2220</td>
<td>USER_PW_CHANGE_FAIL</td>
<td>GSAL.SvcViol</td>
<td>Change of user password failed</td>
</tr>
<tr>
<td>5110</td>
<td>MANUAL_RESET</td>
<td>GSAL.Ina</td>
<td>Manual reset</td>
</tr>
<tr>
<td>5120</td>
<td>RESET_TRIPS</td>
<td>GSAL.Ina</td>
<td>Reset trips</td>
</tr>
<tr>
<td>5130</td>
<td>RESET_LEDS</td>
<td>GSAL.Ina</td>
<td>Reset LEDs</td>
</tr>
<tr>
<td>5270</td>
<td>SYS_STARTUP</td>
<td>GSAL.Ina</td>
<td>System startup</td>
</tr>
<tr>
<td>5280</td>
<td>SYS_SHUTTING_DOWN</td>
<td>GSAL.Ina</td>
<td>System shutting down</td>
</tr>
<tr>
<td>6110</td>
<td>TEST_MODE_START_OK</td>
<td>GSAL.Ina</td>
<td>Test mode started</td>
</tr>
<tr>
<td>6120</td>
<td>TEST_MODE_END</td>
<td></td>
<td>Test mode ended</td>
</tr>
<tr>
<td>6130</td>
<td>CONTRL_OP_PERF_OK</td>
<td></td>
<td>Control operation performed</td>
</tr>
<tr>
<td>6132</td>
<td>CONTRL_OP_PERF_FAIL</td>
<td></td>
<td>Control operation attempt failed</td>
</tr>
</tbody>
</table>

Table continues on next page
<table>
<thead>
<tr>
<th>Event number</th>
<th>Acronyms</th>
<th>GSAL mapping</th>
<th>English</th>
</tr>
</thead>
<tbody>
<tr>
<td>6140</td>
<td>SIGN_FORCED_VALUE</td>
<td></td>
<td>Signal forced — value changed</td>
</tr>
<tr>
<td>7310</td>
<td>HW_CHANGE_DETECTED</td>
<td></td>
<td>Hardware change detected</td>
</tr>
<tr>
<td>8020</td>
<td>DATE_TIME_SET_OK</td>
<td></td>
<td>Date and time set successfully</td>
</tr>
<tr>
<td>8230</td>
<td>NEW_CERT_GEN_FAIL</td>
<td></td>
<td>New certificate generation failed</td>
</tr>
<tr>
<td>9010</td>
<td>ATT_DET_FLOODING</td>
<td></td>
<td>Flooding attack detected</td>
</tr>
<tr>
<td>10010</td>
<td>MAINT_ENTER_MENU_EV</td>
<td></td>
<td>Device entered maintenance menu due to user action</td>
</tr>
<tr>
<td>10020</td>
<td>MAINT_FORCED_MENU_OK</td>
<td></td>
<td>Device successfully forced into maintenance menu due to new state</td>
</tr>
<tr>
<td>10030</td>
<td>MAINT_FTP_ACTIV_OK</td>
<td></td>
<td>FTP server successfully activated from maintenance menu</td>
</tr>
<tr>
<td>10040</td>
<td>MAINT_UPDATE_ABORT_OK</td>
<td></td>
<td>Firmware update procedure aborted successfully</td>
</tr>
<tr>
<td>10050</td>
<td>MAINT_RECOVERY_ENTER_OK</td>
<td></td>
<td>Recovery menu entered successfully</td>
</tr>
<tr>
<td>10052</td>
<td>MAINT_RECOVERY_ENTER_FAIL</td>
<td></td>
<td>Entering Recovery menu failed</td>
</tr>
<tr>
<td>10060</td>
<td>MAINT_AUTH_DIS_FAIL</td>
<td></td>
<td>Authentication disabled from maintenance menu successfully</td>
</tr>
<tr>
<td>10070</td>
<td>MAINT_CHANGE_LOCK_DIS_FAIL</td>
<td></td>
<td>Change lock disabled successfully from Maintenance menu</td>
</tr>
<tr>
<td>10080</td>
<td>MAINT_61850_DIS_OK</td>
<td></td>
<td>IEC 61850 disabled successfully from Maintenance menu</td>
</tr>
<tr>
<td>13200</td>
<td>TRANSFER_CONFIG_OK</td>
<td></td>
<td>Configuration transferred to the device successfully</td>
</tr>
<tr>
<td>13210</td>
<td>TRANSFER_CONFIG_STARTED_OK</td>
<td></td>
<td>Configuration transfer to the device started</td>
</tr>
<tr>
<td>13300</td>
<td>READ_CONFIG_OK</td>
<td></td>
<td>Configuration files read/exported from the device successfully</td>
</tr>
<tr>
<td>13310</td>
<td>READ_CONFIG_STARTED_OK</td>
<td></td>
<td>Configuration exporting from the device started successfully</td>
</tr>
<tr>
<td>13400</td>
<td>TRANSFER_FIRMW_OK</td>
<td></td>
<td>Firmware transferred to the device successfully</td>
</tr>
<tr>
<td>13500</td>
<td>READ_FIRMW_OK</td>
<td></td>
<td>Firmware files read/exported from the device successfully</td>
</tr>
<tr>
<td>13520</td>
<td>TRANSFER_CERTS_OK</td>
<td></td>
<td>Certificates transferred to the device successfully</td>
</tr>
<tr>
<td>13580</td>
<td>READ_CERTS_OK</td>
<td></td>
<td>Exported/read certificates from device successfully</td>
</tr>
<tr>
<td>14200</td>
<td>TRANSFER_CONFIG_FAIL</td>
<td></td>
<td>Failed to transfer configuration to the device</td>
</tr>
<tr>
<td>14300</td>
<td>READ_CONFIG_FAIL</td>
<td></td>
<td>Failed to read configuration files from the device</td>
</tr>
<tr>
<td>14400</td>
<td>TRANSFER_FIRMW_FAIL</td>
<td></td>
<td>Failed to transfer firmware to the device</td>
</tr>
</tbody>
</table>

Table continues on next page
<table>
<thead>
<tr>
<th>Event number</th>
<th>Acronyms</th>
<th>GSAL mapping</th>
<th>English</th>
</tr>
</thead>
<tbody>
<tr>
<td>14500</td>
<td>READ_FIRMW_FAIL</td>
<td></td>
<td>Failed to read firmware files from the device</td>
</tr>
<tr>
<td>14520</td>
<td>TRANSFER_CERTS_FAIL</td>
<td></td>
<td>Failed to transfer certificates to the device</td>
</tr>
<tr>
<td>14580</td>
<td>READ_CERTS_FAIL</td>
<td></td>
<td>Failed to read certificates from the device</td>
</tr>
</tbody>
</table>
Section 6  Local HMI use

At delivery, logging on is not required and the user has full access until users and passwords are created with PCM600 and written into the IED. The LHMI is logged on as SuperUser by default until other users are defined.

Commands, changing parameter values and resetting indications, for example, are actions requiring password when the password protection is activated. Reading information on the LHMI is always allowed without password. The LHMI is logged on as Guest by default when other users are defined.

Utility security policies and practical consideration should always be taken on the feasibility of using passwords. In emergency situations, the use of passwords could delay urgent actions. When security issues must be met, the two factors must be seriously considered.

The auxiliary power supply to the IED must not be switched off before changes such as passwords, setting parameter or local/remote control state changes are saved.

6.1  Logging on

1. Press \[
\text{to activate the logon procedure.}
\]
The logon is also activated when attempting a password-protected operation.
2. Select the user name by scrolling with \[
\text{and } \text{.}
\]

![Figure 21: Selecting the user name](IEC12000161-2-en.vsd)

3. Enter the password when prompted and select OK.
Activate the character to be entered with ▲ and ▼.
Enter the character with ▲ and ▼.

Upper and lower case letters are also found by scrolling the 255 characters with ▲ and ▼.

**Main menu**
- Control
- Events
- Measurements
- Disturbance records
- Settings
- Configuration
- Diagnostics
- Tests
- Clear
- Languages

<table>
<thead>
<tr>
<th>User</th>
<th>Password</th>
</tr>
</thead>
<tbody>
<tr>
<td>johnsmith</td>
<td>***********</td>
</tr>
<tr>
<td>Log on</td>
<td>OK Cancel</td>
</tr>
</tbody>
</table>

2013-03-13 20:55:44 Guest Object name

*Figure 22: Entering the password*

Passwords are case sensitive.

**Only characters A - Z, a - z and 0 - 9 shall be used in user names. User names are not case sensitive. For passwords see the Password policies in PCM600.**

4. Press ▼ to confirm the logon or ▲ to cancel the procedure. If the logon fails, a message is displayed on the display.
Once a user is created and written into the IED, logon is possible with the password assigned in the tool. If there is no user created, an attempt to log on causes the display to show a corresponding message.

**Figure 23: Error message indicating an incorrect password**

The logon dialog appears if the attempted operation requires another level of user rights.

**Figure 24: No user defined**

### 6.2 Logging off

The user is automatically logged off after the display timeout. The IED returns to a state where only reading is enabled. Manual logoff is also possible.
1. Press 🛑.
2. To confirm logoff, select Yes and press 🛑.

![Main menu]

- Configuration
- Diagnostics
- Tests
- Clear
- Languages

<table>
<thead>
<tr>
<th>2013-03-13 21:12:45</th>
<th>johnsmith</th>
<th>Object name</th>
</tr>
</thead>
</table>

IEC12000159-2-en.vsd

Figure 25: Logging off

* To cancel logoff, press 🛑.

### 6.3 Saving settings

Editable values are stored in the nonvolatile flash memory. Most of the parameter changes take effect immediately after storing, but some parameter changes require application restart. Values stored in the flash memory remain in effect also after reboot.

1. Press 🛑 to confirm any changes.
2. Press 🛑 to move upwards in the menu tree or 🛑 to enter the Main Menu.
3. To save the changes in nonvolatile memory, select Yes and press 🛑.

![Monitoring]

Save changes?
Setting group: 1
🚦 No Cancel

<table>
<thead>
<tr>
<th>2013-03-25 07:23:31</th>
<th>johnsmith</th>
<th>Object name</th>
</tr>
</thead>
</table>

IEC12000164-2-en.vsd

Figure 26: Confirming settings
6.4 Recovering password

In case of password loss or any other file system error that prevents the IED from working properly, the whole file system can be restored to IED default state. All the default settings and configuration files stored in the IED at the factory are restored. One important usage of this menu is to disable the authority system. This can be used to recover an IED where the user-defined passwords are lost.

It is possible to disable the Maintenance menu. This is done by setting the parameter `MaintMenuEnable` to `No` in the Group `AUTHMAN: 1` using the Parameter settings in PCM600.

If the Maintenance menu is disabled, there is no way to bypass authority if passwords are forgotten. To be able to do field updating, the maintenance menu have to be re-enabled.

To enter this menu, the IED must be rebooted and a specific key combination must be pressed on the LHMI during the IED boot sequence.

1. Switch off the power supply to the IED and leave it off for one minute.
2. Switch on the power supply to the IED and press and hold down `?` and `?` until the Maintenance Menu appears on the LHMI (this takes around 20-60s).
Figure 27: Select Recovery menu

4. Enter PIN code 8282 and press ".

Figure 28: Enter PIN code

5. Select Turn off authority and press or .
Figure 29: Turn off Authority

6. Select OK to turn off the authority and press .

Figure 30: Confirm selection

7. Press to continue the startup sequence, (now the authority is temporarily disabled until next reboot of the IED).

To cancel the operation in any step, press ESC.

Open PCM600 and start the IED Users tool.

- Remove the faulty user
- Create a new user with the same access rights
- Write the user management settings to the IED

The IED perform a reboot, new settings are activated and the authority system is enabled again.
The Maintenance Menu is only available on the Local HMI. The purpose of this menu is to have a way to recover in the field at different situations. The recovery menu is also protected with a 4-digit PIN code, fixed for all IEDs.

Avoid unnecessary restoring of factory IED default setting (Revert to IED defaults), since all parameter settings earlier written to the IED are overwritten with factory default values.

When Revert to IED defaults is selected the IED restores the factory IED default settings and restarts. Restoring can take several minutes. Confirmation of the restored factory IED default settings is shown on the display for a few seconds, after which the IED restarts.
### Section 7  IEEE Compliance statement

#### 7.1 IEEE1686 compliance

<table>
<thead>
<tr>
<th>Clause</th>
<th>Title</th>
<th>Status</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>IED cyber security features</td>
<td>Acknowledge</td>
<td></td>
</tr>
<tr>
<td>5.1</td>
<td>Electronic access control</td>
<td>Comply</td>
<td>Access is protected for local access through control panel. Access is protected for local access through a communication /diagnostic port. Access is protected for remote access through a communication media</td>
</tr>
<tr>
<td>5.1.1</td>
<td>Password defeat mechanisms</td>
<td>Comply</td>
<td>20 unique ID/password combinations are supported</td>
</tr>
<tr>
<td>5.1.2</td>
<td>Number of individual ID/passwords supported</td>
<td>Comply</td>
<td>The minimum enforced password length is configurable. If password policy is enforced, minimum is 6. Use of mix of lower and UPPERCASE characters is enforced, configurable in password policies Use of numerical values is enforced, configurable in password policies. Use of non-alphanumeric character (e.g. @, #, %, *) is enforced, configurable in password policies</td>
</tr>
<tr>
<td>5.1.3</td>
<td>Password construction</td>
<td>Comply</td>
<td>View data feature is accessible through individual user accounts</td>
</tr>
<tr>
<td>5.1.4</td>
<td>Authorization levels by password</td>
<td>Comply</td>
<td>View configuration settings feature is accessible through individual user accounts</td>
</tr>
<tr>
<td>5.1.4.1</td>
<td>View data</td>
<td>Comply</td>
<td>Force value feature is accessible through individual user accounts</td>
</tr>
<tr>
<td>5.1.4.2</td>
<td>View configuration settings</td>
<td>Comply</td>
<td>Configuration feature is accessible through individual user accounts</td>
</tr>
<tr>
<td>5.1.4.3</td>
<td>Force values</td>
<td>Comply</td>
<td>User account (ID / password) management feature is accessible through individual user accounts</td>
</tr>
<tr>
<td>5.1.4.4</td>
<td>Configuration change</td>
<td>Comply</td>
<td>Audit log view / download feature is accessible through individual user accounts</td>
</tr>
<tr>
<td>5.1.4.5</td>
<td>Firmware change</td>
<td>Comply</td>
<td></td>
</tr>
<tr>
<td>5.1.4.6</td>
<td>ID/password management</td>
<td>Comply</td>
<td></td>
</tr>
<tr>
<td>5.1.4.7</td>
<td>Audit log</td>
<td>Comply</td>
<td></td>
</tr>
<tr>
<td>5.1.5</td>
<td>Password display</td>
<td>Comply</td>
<td></td>
</tr>
<tr>
<td>Clause</td>
<td>Title</td>
<td>Status</td>
<td>Comment</td>
</tr>
<tr>
<td>----------</td>
<td>----------------------------------------------</td>
<td>----------</td>
<td>-------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>5.1.6</td>
<td>Access time-out</td>
<td>Comply</td>
<td>A time-out feature exists. The time period is configurable by the user.</td>
</tr>
<tr>
<td>5.2</td>
<td>Audit trail</td>
<td>Comply</td>
<td>The Audit log can be viewed through PCM 600</td>
</tr>
<tr>
<td>5.2.1</td>
<td>Storage capability</td>
<td>Comply</td>
<td></td>
</tr>
<tr>
<td>5.2.2</td>
<td>Storage record</td>
<td>Comply</td>
<td></td>
</tr>
<tr>
<td>5.2.2.1</td>
<td>Event record number</td>
<td>Comply</td>
<td></td>
</tr>
<tr>
<td>5.2.2.2</td>
<td>Time and date</td>
<td>Comply</td>
<td></td>
</tr>
<tr>
<td>5.2.2.3</td>
<td>User ID</td>
<td>Comply</td>
<td></td>
</tr>
<tr>
<td>5.2.2.4</td>
<td>Event type</td>
<td>Comply</td>
<td></td>
</tr>
<tr>
<td>5.2.3</td>
<td>Audit trail event types</td>
<td>Comply</td>
<td></td>
</tr>
<tr>
<td>5.2.3.1</td>
<td>Login</td>
<td>Comply</td>
<td></td>
</tr>
<tr>
<td>5.2.3.2</td>
<td>Manual logout</td>
<td>Comply</td>
<td></td>
</tr>
<tr>
<td>5.2.3.3</td>
<td>Timed logout</td>
<td>Comply</td>
<td></td>
</tr>
<tr>
<td>5.2.3.4</td>
<td>Value forcing</td>
<td>Comply</td>
<td></td>
</tr>
<tr>
<td>5.2.3.5</td>
<td>Configuration access</td>
<td>Comply</td>
<td></td>
</tr>
<tr>
<td>5.2.3.6</td>
<td>Configuration change</td>
<td>Comply</td>
<td></td>
</tr>
<tr>
<td>5.2.3.7</td>
<td>Firmware change</td>
<td>Comply</td>
<td></td>
</tr>
<tr>
<td>5.2.3.8</td>
<td>ID/password creation or modification</td>
<td>Comply</td>
<td></td>
</tr>
<tr>
<td>5.2.3.9</td>
<td>ID/password deletion</td>
<td>Comply</td>
<td></td>
</tr>
<tr>
<td>5.2.3.10</td>
<td>Audit-log access</td>
<td>Comply</td>
<td></td>
</tr>
<tr>
<td>5.2.3.11</td>
<td>Time/date change</td>
<td>Comply</td>
<td></td>
</tr>
<tr>
<td>5.2.3.12</td>
<td>Alarm incident</td>
<td>Comply</td>
<td></td>
</tr>
<tr>
<td>5.3</td>
<td>Supervisory monitoring and control</td>
<td>Comply</td>
<td></td>
</tr>
<tr>
<td>5.3.1</td>
<td>Events</td>
<td>Exception</td>
<td>Automated time changes and read of configuration are not reported; otherwise compliance</td>
</tr>
<tr>
<td>5.3.2</td>
<td>Alarms</td>
<td>Exception</td>
<td>No Client certificates are in use</td>
</tr>
<tr>
<td>5.3.2.1</td>
<td>Unsuccessful login attempt</td>
<td>Comply</td>
<td></td>
</tr>
<tr>
<td>5.3.2.2</td>
<td>Reboot</td>
<td>Comply</td>
<td></td>
</tr>
<tr>
<td>5.3.2.3</td>
<td>Attempted use of unauthorized configuration software</td>
<td>Exception</td>
<td>Not supported</td>
</tr>
<tr>
<td>5.3.2.4</td>
<td>Alarm point change detect</td>
<td>Comply</td>
<td></td>
</tr>
<tr>
<td>5.3.4</td>
<td>Event and alarm grouping</td>
<td>Exception</td>
<td>Not supported</td>
</tr>
<tr>
<td>5.3.5</td>
<td>Supervisory permissive control</td>
<td>Exception</td>
<td>Not supported</td>
</tr>
<tr>
<td>5.4</td>
<td>Configuration software</td>
<td>Acknowledge</td>
<td></td>
</tr>
<tr>
<td>5.4.1</td>
<td>Authentication</td>
<td>Exception</td>
<td>Configuration download is handled by authentication</td>
</tr>
<tr>
<td>5.4.2</td>
<td>ID/password control</td>
<td>Comply</td>
<td></td>
</tr>
<tr>
<td>5.4.3</td>
<td>ID/password-controlled features</td>
<td>Comply</td>
<td></td>
</tr>
<tr>
<td>5.4.3.1</td>
<td>View configuration data</td>
<td>Comply</td>
<td></td>
</tr>
</tbody>
</table>

Table continues on next page
<table>
<thead>
<tr>
<th>Clause</th>
<th>Title</th>
<th>Status</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.4.3.2</td>
<td>Change configuration data</td>
<td>Comply</td>
<td></td>
</tr>
<tr>
<td>5.4.3.3</td>
<td>Full access</td>
<td>Comply</td>
<td></td>
</tr>
<tr>
<td>5.5</td>
<td>Communications port access</td>
<td>Comply</td>
<td></td>
</tr>
<tr>
<td>5.6</td>
<td>Firmware quality assurance</td>
<td>Exception</td>
<td>Quality control is handled according to ISO9001 and CMMI.</td>
</tr>
</tbody>
</table>
Section 8 Glossary

AES
Advanced Encryption Standard (AES) is a specification for the encryption of electronic data. The key size used for an AES cipher specifies the number of repetitions of transformation rounds that convert the input, called the plaintext, into the final output, called the ciphertext. The number of cycles of repetition are as follows: 10 cycles of repetition for 128-bit keys, 12 cycles of repetition for 192-bit keys, 14 cycles of repetition for 256-bit keys.

AGSAL
Generic security application

ANSI
American National Standards Institute

ASCII
American Standard Code for Information Interchange (ASCII) is a character-encoding scheme originally based on the English alphabet. ASCII codes represent text in computers, communications equipment, and other devices that use text.

CA
In cryptography, certificate authority, or certification authority, (CA) is an entity that issues digital certificates. The digital certificate certifies the ownership of a public key by the named subject of the certificate

CMT
Communication Management tool in PCM600

CPU
Central processor unit

CRC
Cyclic redundancy check

DARPA
Defense Advanced Research Projects Agency (The US developer of the TCP/IP protocol etc.)

DHCP
Dynamic Host Configuration Protocol

DNP3
DNP3 (Distributed Network Protocol) is a set of communications protocols used between components in process automation systems. Its main use is in utilities such as electric and water companies. It plays a crucial role in SCADA systems, where it is used by SCADA Master Stations (aka Control Centers), Remote Terminal Units (RTUs), and Intelligent Electronic Devices (IEDs). It is primarily used for communications between a master station and RTUs or IEDs’.

EMC
Electromagnetic compatibility

EN 50263
Electromagnetic compatibility (EMC) - Product standard for measuring relays and protection equipment.

EN 60255-26
Electromagnetic compatibility (EMC) - Product standard for measuring relays and protection equipment.

EN 60255-27
Electromagnetic compatibility (EMC) - Product standard for measuring relays and protection equipment.

ESD
Electrostatic discharge

FTP
File Transfer Protocol (FTP) is a standard network protocol used to transfer files from one host or to another host over a TCP-based network, such as the Internet.

FTPS
FTPS (also known as FTP-ES, FTP-SSL and FTP Secure) is an extension to the commonly used File Transfer Protocol (FTP) that adds support for the Transport Layer Security (TLS) and the Secure Sockets Layer (SSL) cryptographic protocols.

GDE
Graphical display editor within PCM600

GOOSE
Generic object-oriented substation event

GPS
Global positioning system
<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>GSM</td>
<td>GPS time synchronization module</td>
</tr>
<tr>
<td>GTM</td>
<td>GPS Time Module</td>
</tr>
<tr>
<td>HMI</td>
<td>Human-machine interface</td>
</tr>
<tr>
<td>ID</td>
<td>IDentification</td>
</tr>
<tr>
<td>IEC</td>
<td>International Electrical Committee</td>
</tr>
<tr>
<td>IEC 60255</td>
<td>This standard specifies the general performance requirements of all electrical measuring relays and protection equipment used in the electrotechnical fields covered by the IEC.</td>
</tr>
<tr>
<td>IEC 60870-5-103</td>
<td>Communication standard for protective equipment. A serial master/slave protocol for point-to-point communication</td>
</tr>
<tr>
<td>IEC 61850</td>
<td>Substation automation communication standard</td>
</tr>
<tr>
<td>IEC 61850–8–1</td>
<td>Communication protocol standard</td>
</tr>
<tr>
<td>IED</td>
<td>Intelligent electronic device</td>
</tr>
<tr>
<td>IEDUM</td>
<td>IED User Management</td>
</tr>
<tr>
<td>IEEE</td>
<td>Institute of Electrical and Electronics Engineers</td>
</tr>
<tr>
<td>IEEE1686</td>
<td>Standard for Substation Intelligent Electronic Devices (IEDs') Cyber Security Capabilities</td>
</tr>
</tbody>
</table>
| IP           | 1. Internet protocol. The network layer for the TCP/IP protocol suite widely used on Ethernet networks. IP is a connectionless, best-effort packet-switching protocol. It provides packet routing, fragmentation and reassembly through the data link layer.  
2. Ingression protection, according to IEC standard |
| IP 20        | Ingression protection, according to IEC standard, level 20 |
| ISO 9001     | Set of standards for quality management. |
| IT           | Information technology |
| LAN          | Local area network |
| LED          | Light-emitting diode |
| LHMI         | Local Human Machine Interface, also Local HMI. |
| MicroSCADA   | System for supervision, control and data acquisition |
| NCC          | National Control Centre |
| ODBC         | Open Database Connectivity is a standard for accessing database management systems (DBMS). |
| PC           | Personal Computer |
| PCI          | Peripheral component interconnect, a local data bus |
| PCM600       | Protection and control IED manager |
| PIN          | Personal Identification Number |
| PST          | Parameter setting tool within PCM600 |
| RTU          | Remote terminal unit |
| SA           | Substation Automation |
| SCADA        | Supervision, control and data acquisition, see also MicroSCADA |
| SCT          | System configuration tool according to standard IEC 61850 |
| SHA          | The Secure Hash Algorithm is a family of cryptographic hash functions. The SHA 2 family comprise two similar hash functions, with different block sizes, known as SHA-256 and SHA-512. |
**SMT**
Signal matrix tool within PCM600

**SNTP**
Simple network time protocol – is used to synchronize computer clocks on local area networks. This reduces the requirement to have accurate hardware clocks in every embedded system in a network. Each embedded node can instead synchronize with a remote clock, providing the required accuracy.

**SPA**
Strömberg protection acquisition, a serial master/slave protocol for point-to-point communication

**SSL/TLS**
Transport Layer Security (TLS) and its predecessor, Secure Sockets Layer (SSL), are cryptographic protocols that provide communication security over the Internet. TLS and SSL encrypt the segments of network connections at the Application Layer for the Transport Layer, using asymmetric cryptography for key exchange, symmetric encryption for confidentiality, and message authentication codes for message integrity.

**Syslog**
Syslog is a standard for computer data logging. Syslog can be used for computer system management and security auditing as well as generalized informational, analysis, and debugging messages

**TCP**
Transmission control protocol. The most common transport layer protocol used on Ethernet and the Internet.

**TCP/IP**
Transmission control protocol over Internet Protocol. The de facto standard Ethernet protocols incorporated into 4.2BSD Unix. TCP/IP was developed by DARPA for Internet working and encompasses both network layer and transport layer protocols. While TCP and IP specify two protocols at specific protocol layers, TCP/IP is often used to refer to the entire US Department of Defense protocol suite based upon these, including Telnet, FTP, UDP and RDP.

**UDP**
The User Datagram Protocol (UDP) is one of the core members of the Internet protocol suite. With UDP, computer applications can send messages, in this case referred to as datagrams, to other hosts on an Internet Protocol (IP) network without prior communications to set up special transmission channels or data paths.

**UMT**
User management tool

**UTC**
Coordinated Universal Time. A coordinated time scale, maintained by the Bureau International des Poids et Mesures (BIPM), which forms the basis of a coordinated dissemination of standard frequencies and time signals. UTC is derived from International Atomic Time (TAI) by the addition of a whole number of “leap seconds” to synchronize it with Universal Time 1 (UT1), thus allowing for the eccentricity of the Earth’s orbit, the rotational axis tilt (23.5 degrees), but still showing the Earth’s irregular rotation, on which UT1 is based. The Coordinated Universal Time is expressed using a 24-hour clock, and uses the Gregorian calendar. It is used for aeroplane and ship navigation, where it is also sometimes known by the military name, "Zulu time." "Zulu" in the phonetic alphabet stands for "Z", which stands for longitude zero.

**VPN**
A Virtual Private Network (VPN) extends a private network across public networks like the Internet. It enables a host computer to send and receive data across shared or public networks as if it were a private network with all the functionality, security and management policies of the private network.