TROUBLESHOOTING GUIDE

High PROTEC | TROUBLESHOOTING GUIDE

Version: 3.7

Original document

English

REFERENCE MANUAL HPT-3.7-EN-TSG | Revision A
Build 50882

Original reference manual

SEG Electronics GmbH

Krefelder Weg 47 • D–47906 Kempen (Germany)

Telephone: +49 (0) 21 52 145 1

Internet: www.SEGelectronics.de

Sales

Telephone: +49 (0) 21 52 145 331

Fax: +49 (0) 21 52 145 354

E-mail: sales@SEGelectronics.de

Service

Telephone: +49 (0) 21 52 145 614

Fax: +49 (0) 21 52 145 354

E-mail: support@SEGelectronics.de

Table of Contents

1   Self-Supervision Messages

The protection device supervises its normal operation by executing various self-supervision checks during runtime of the device.

When the protection device has detected a problem, the system LED starts flashing alternating red and green, and a message is recorded in the internal memory.

Please check the self-supervision messages under [Operation / Self-Supervision / Messages].

Furthermore, the following messages are directly related to IT security:

SE 37, SW 6, SW 7, SW 8, SI 4, SI 5, SI 7, SI 9, SI 10.

These security-related messages can also be viewed at the menu path [Operation / Security / Security Logger].

1.1   Self-Supervision – Error Messages

Description	Information	Corrective Action
SE 1 *Abort*	*The device underwent an unscheduled restart.*	Get in contact with our service-team. You will be supplied with a tool for error analysis.
SE 2…4 *Problem w. resources*	*Critical level of internal resources. It is not possible for the user to take any actions.*	Get in contact with our service-team. You will be supplied with a tool for error analysis.
SE 5…10	*– reserved for future use –*	—
SE 11 *FRAM defective*	*Hardware: FRAM defect. The device will be set out-of-service on next reboot, and it will have to be sent for repair.*	Send the device for repair.
SE 12 *Battery low*	*The battery for buffering the real time clock is low.*	The battery can be exchanged by the manufacturer. There's no impact on the functionality of the device if the battery breaks down, except for the buffering of the clock while the unit is in de-energized condition.
SE 13…14	*– reserved for future use –*	—
SE 15 *Problem w. resources*	*Critical level of internal resources. It is not possible for the user to take any actions.*	Get in contact with our service-team. You will be supplied with a tool for error analysis.

Description	Information	Corrective Action
SE 16…29	*– reserved for future use –*	—
SE 30 *Prot Comm Err*	*Problems with the 24 km Line Differential module.*	Get in contact with our service-team. You will be supplied with a tool for error analysis.
SE 31 *Intern. config.*	*There is a critical internal fault. It is not possible for the user to take any actions.*	Get in contact with our service-team.
SE 32 *Prot Comm Err*	*Problems with the 24 km Line Differential module.*	Get in contact with our service-team.
SE 33 *Prot Comm Err*	*Problems with the Line Differential protection communication.*	Get in contact with our service-team.
SE 34 (= S 34)	*– only until Firmware-Release 3.4 –*	As of Firmware-Release 3.6, this has been moved to SW 9.
SE 35…36	*– reserved for future use –*	—
SE 37 *Inval TLS cert.*	*The certificate for the encrypted communication is invalid.*	Get in contact with our service-team.

1.2　　Self-Supervision – Warning Messages

Description	Information	Corrective Action
SW 1…3	*– reserved for future use –*	—
SW 4　*Power Supply*	*Your device suffered a short-term sag or outage of the supply voltage.*	Check your power supply.
SW 5　*No time sync*	*Warning that the device is operating without time synchronization.*	If the missing time synchronization is intentional this warning can be safely ignored. Otherwise, you should check the synchronization settings and connection (e. g. for IRIG-B).
SW 6　*TLS basic cert.*	*The device uses a basic certificate for the encrypted communication. Compared with a device-specific certificate, this means a slightly reduced security level.*	The basic certificate is installed when an old firmware, that did not support encrypted communication, is updated by the user. A device-specific certificate, however, can be installed by the manufacturer.
SW 7	*– reserved for future use –*	—
SW 8　*Mult. inval. Conn. Pwd*	*Warning that a wrong connection password was entered multiple times in series.*	The message value is the number of wrong password entries in series. It gets reset to 0 (warning end) when the connection password is entered correctly (and also with a restart of the device). You should check whether this indicates an unauthorized access attempt (as the connection password is needed to establish a *Smart view* connection).
SW 9　*Disturb Rec Trigger*	*Perpetual trigger of the Disturbance Recorder. Too many records created during a monitored time span.*	Make sure that the Disturbance Recorder is not triggered too frequently. Check the following settings: • Configuration of the Disturbance Recorder: Verify that each of the defined trigger sources is configured by intention. • In the Event Recorder you can see which protection function creates excessive events (as trigger for the Disturbance Recorder). Check the settings of this protection function, especially the alarm levels. Adapt them, if necessary. • Device planning: Make sure that no superfluous protection functions are projected that you do not need.

Description	Information	Corrective Action
		See also "The Disturbance Recorder is permanently logging new records".
SW 10 *Connection refused*	*The protection device refused an incoming connection because of certificate or encryption problems.*	This message typically results from a connection attempt using some illegal client software (i. e. other than *Smart view*). You should check whether this indicates an unauthorized access attempt.
SW 11 *IEC104 queue overfl.*	*There were more IEC104-related events generated than could be handled. This resulted in an IEC104 queue overflow and corrupt internal IEC104 data, so that the IEC104 protocol has been disabled automatically. It can be re-enabled by resetting the counters at [Operation/Reset] »IEC104 . Res all Diag Cr«.*	This message should not occur except in very uncommon stress situations. Therefore we recommend to get in contact with our service-team.

1.3   Self-Supervision – Information Messages

Description	Information	Corrective Action
SI 1…3	*– reserved for future use –*	—
SI 4 *Inval Password*	*Information that a wrong (access level) password was entered.*	The message value is the number of wrong passwords that have been entered within some time.
SI 5 *Inval Conn. Pwd*	*Information that a wrong connection password was entered.*	The message value is the number of wrong connection passwords that have been entered within some time.
SI 6 *Settings changed*	*Information that the settings (e.g. the protection parameters) have been modified.*	The message value is the number of setting changes that have been made within some time. (A setting change is counted whenever new parameter values are transferred to the device or saved at the HMI panel.)
SI 7 *Firmware Update*	*Information that a new device firmware has been installed.*	
SI 8 *Device restart*	*Information that the device has been restarted.*	The message value shows the reason for the device restart. Device Start-up Codes: 1=Normal Start-up; 2=Reboot by the Operator; 3=Reboot by means of Super Reset; 4=outdated; 5=outdated; 6=Unknown Error Source; 7=Forced Reboot (initiated by the main processor); 8=Exceeded Time Limit of the Protection Cycle; 9= Forced Reboot (initiated by the digital signal processor); 10=Exceeded Time Limit of the Measured Value Processing; 11=Sags of the Supply Voltage; 12=Illegal Memory Access.
SI 9 *Remote Access*	*Information that a Smart view connection via network (e.g. Ethernet) has been established.*	
SI 10 *Password changed*	*Information that a password has been changed by the user.*	The message value is the number of password changes that have been made within some time.

Troubleshooting Guide

2   System LED Signals

Off (Not Illuminated)

Description	Information	Corrective Action
The **System LED is off** (not illuminated), and the other LEDs are also off.	Either no supply voltage or the power supply is faulty.	Please check the supply voltage. If it is OK, send the device to be repaired.

Undefined, Not Flashing

Description	Information	Corrective Action
The **System LED is undefined and not flashing**, and the other LEDs are showing a random pattern.	The CPU board is faulty.	Send the device to be repaired.

Flashing Red

Description	Information	Corrective Action
The **System LED is flashing red** and the HMI shows an error number.	Fatal system error.	Get in contact with our service-team.

Constantly Red

Description	Information	Corrective Action
The **System LED is constantly red** and the HMI shows an error number.	Fatal system error.	Get in contact with our service-team.
You have started the device while pressing the »CTRL« key.	This is not a device error but the normal activity for performing a bootloader or firmware update.	Please follow the instructions for installing an update.

Flashing Green

Description	Information	Corrective Action
The **System LED is flashing green**, and after some time it changes to constantly green.	This is not a device error but the normal start-up phase. As soon as the System LED changes to constantly green, the protection functions are active.	The LED should have changed to constantly green after approx. 30 seconds.

Flashing Red/Green

Description	Information	Corrective Action
The **System LED is flashing red+green**.	The device is operating and all protection functions are working. But the internal self-supervision module has detected a previous problem in the system, which has been recorded as a Self-Supervision message.	Please check the Self-Supervision messages (see ⤷ "1 Self-Supervision Messages"), or get in contact with our service-team. You can acknowledge the flashing System LED under [Operation / Acknowledge] »SSV . Ack System LED «.

Constantly Green

Description	Information	Corrective Action
The **System LED is constantly green**, but the device's HMI is not operable. There are no Softkeys shown on the panel. Instead the panel shows „Startup" or just the device type (e. g. MCA4) without any Softkeys.	The device is starting up. The protection functions are already working, but the HMI is still starting up. If this is not finished after 5 minutes, the device is probably busy with handling Ethernet packets (Connector X100).	Check if the following action makes the device´s HMI operable: Plug off the Ethernet (Connector X100). If the HMI is getting operable, there is an error on your Ethernet network (e. g. an Ethernet storm). Please check your network traffic.
The **System LED is constantly green**, but the device's HMI is not operable. A normal page of the HMI is visible: Either there are Softkeys visible or the LED status page is being displayed.	The device is busy with handling Ethernet packets (Connector X100). The protection functions are working.	Plug off the Ethernet (Connector X100). If the HMI is getting operable, there is an error on your Ethernet network (e. g. an Ethernet storm). Please check your network traffic. If this action does not change the behavior of the device try to follow the next troubleshooting entry.
The **System LED is constantly green**, but the device's HMI is not operable. A normal page of the HMI is visible: Either there are Softkeys visible or the LED status page is being displayed. There is no Ethernet connector (Connector X100).	Some of the system parts are not working. The protection functions, however, are working.	Keep the device running and connected to the supply voltage. Get in contact with our service-team. You will be supplied with a tool for error analysis.
The device's **HMI is operable**.	This is not a device error. The device is ready for operation and protects your electrical equipment. If you have the impression that the relay is not working correctly or you have any problems with setting the parameters, please check the next troubleshooting entries.	—

3 Problems with the Device

3.1 Hardware

Description	Information	Corrective Action
Display failure.	*After selecting any key, the whole display remains dark or the display is defective.*	Check the following issues: • Is the supply voltage connected? This is the case when the System LED is illuminated. • Is the environmental temperature within the allowed range? • Try to adjust (increase / decrease) the contrast of the display by using *Smart view*. • If all these checks do not yield any results, send the device back to the manufacturer.
Failure of a binary output.	*The physical status does not match the reported state, as it is being shown via HMI or Smart view.*	Check the following issues: • Is the binary output in latched state? If yes, acknowledge (reset) the latching. • Is the inverting parameter *»Inverting«* set to "active" for the particular binary output? • Check the wiring. • Disconnect the wiring from the binary output and measure the output voltage. Set the state of the binary output by using the test functions Force / Disarm (see Technical Manual). • See also the entry Binary outputs do not react. • If all these checks do not yield any results, send the device back to the manufacturer.
Failure of a binary input.	*The physical status does not match the reported state, as it is being shown via HMI or Smart view.*	Check the following issues: • Is the configured voltage level set correctly? • Is the voltage level of the digital input (i. e. the signal level) correct? • Is the inverting parameter set? • Check the wiring. • If all these checks do not yield any results, send the device back to the manufacturer.

Description	Information	Corrective Action
Wrong setting of the system time *after an outage of the supply voltage.*	*The internal battery for powering the clock during an outage of the supply voltage is empty or defect.*	The device is working properly with an empty clock battery. The system time can be synchronized externally. Nevertheless you might want to have the battery replaced. Please contact the service-team.
Failure of a key.		Send the device back to the manufacturer.
Only for Line Differential devices: **Failure of the fiber optic port**.		Verify the correct functionality of the fiber optic module by performing a loopback test: • Build a short direct connection between the RX and TX ports of the fiber optic interface. • During the loopback test, the device sends and receives its own data, as if the data were sent by the remote device. Therefore the differential protection modules, the Transfer Trip module or the Signal Transfer module might trip during this test! Therefore we recommend to block these modules (or their trip commands) during the test. The fiber optic module is functioning if the following is fulfilled: • The value of [Operation / Status Display / Prot-Transfer / ProtCom / Advanced States] »Operating Mode« is "Loopback". • The counter [Operation / Status Display / Prot-Transfer / ProtCom / State] »24h Err Cr« shows some constant value.

3.2 Operation of the Device

Description	Information	Corrective Action
The **binary outputs or LEDs are in unexpected state**.	A binary output or an LED has been reconfigured from latched to unlatched.	Only until Release 3.5: The status of the binary output / LED must be acknowledged once, if it had already been pending before the reconfiguration. (As of Release 3.6, no action is required.) Independent of this, note that the set value of »*t-Off Delay*« has to elapse before the binary outputs / LEDs will change their state. Moreover, note that a latched state even »survives« a restart of the device.
Missing **text-labels (with the description of the LED assignments)** on the device front.		There is a template as a PDF file, named „HighPROTEC_Inserts_Bx.pdf". This can be adapted and printed out on adhesive labels. The file is available on the (separately available) product DVD. Moreover it can be directly downloaded from a dedicated web address that is printed (as URL and QR code) on a sticker glued to the housing of the device.
The device is set to the **wrong language (e. g. English)**.	All HighPROTEC devices are shipped with English language being pre-set. You can select a different language at any time.	Connect the relay to the supply voltage. After the relay has completely booted, select [Device Para / HMI] »*Menu language*« on the HMI and select a different language.
Smart view is set to the **wrong language (e. g. English)**.	You have installed Smart view with English language. Now you want to switch to a different language.	Select [Settings / Language] within *Smart view* and select your desired language. A window will pop up. This informs you that the language will get activated after a restart of *Smart view*. Accept this information, close and restart *Smart view*.
It is required to be able to **acknowledge a latched LED without entering a password**.		As of HighPROTEC Release 3.6, the feature "Immediate Acknowledgment by a Long Keypress" is set by default in a way such that LEDs can be acknowledged (reset) by pressing the »C« key for approx. 1 second, and this works *without* any password entry. See the chapter "Acknowledgments" in the Technical Manual.
It is required to be able to **acknowledge a latched trip without entering a password**.		Define a blank password for the access level **Prot-Lv1**. For a blank password, there is no password query for this access level. But be aware that there are more settings associated with this access level.

Description	Information	Corrective Action
		You can find a general description of access levels in chapter "Security" of the Technical Manual. Moreover, the Reference Manual lists all parameters in tabular form with their respective access level.
What is the default password?		The factory-provided default passwords are as follows • Access level passwords: "**1234**". • Connection passwords (as of HighPROTEC Release 3.6): blank. (See the chapter "Security" in the Technical Manual.)
How do I reset the password?		Refer to the section "Password Forgotten" within the "Security" chapter of the Technical Manual.
The **connection password does not work**.	*You have entered the wrong connection password.*	There is a password *»USB connection«* for the connection via the USB interface, and there is another password *»Remote network connection«* for a connection via network.
Which **restrictions exist for an access-level password**?		The rules for an access-level password are as follows: • only the digits 1, 2, 3, 4. • max. 8 digits.
Which **restrictions exist for a connection password**?		The rules for a connection password are different from an access-level password: • A connection password may be long (even more than 64 characters). • A connection password may contain all printable (Unicode) characters, incl. blanks.

3.3 Parameter Settings

Description	Information	Corrective Action
Problems with the **transfer of device parameters** *from one protection device to another of the same type (e. g. MCA4).*	*You have configured the parameters of a Troubleshooting_HPT device. Now you want to transfer these parameters to another device. This is possible if both devices are of the same type, e. g. MCA4.*	Read out the device parameters with *Smart view* from the first device. Save them into a file. Now reopen this file with *Smart view*. Adapt the settings to the order code of the second device by selecting [Edit / Modify Device Configuration (Typecode)…]. Select »Apply«. By this the existing parameter file is being converted to the format of the second device. Now there may be implausible parameters. These are marked with a question mark and are not valid for this device type. Please adapt the values of the implausible parameters. Afterwards you can transfer the parameter settings to the second device.
All **parameter changes are refused** *with the message "Please wait\nSystem locked".*	*All parameter changes, including the transfer of parameters to a protection device, are refused with the message "Please wait\nSystem locked" on the device´s display (or a comparable message by Smart view) – The protection device is locked against parameter changes.*	There are two potential reasons why parameter changes might be locked: • An intentional setting lock has been activated by assigning a signal to [Field Para / General Settings] *»Setting Lock«*. The setting lock is released as soon as the assigned signal becomes "inactive". If it is not possible to set that signal inactive you can temporarily bypass the setting lock at [Field Para / General Settings] *»Setting Lock Bypass«*. • A switching operation is ongoing (or at least the protection device believes this). In general, parameter changes are refused during a switching operation. Switching operations should last only for a short time. So, if setting changes are refused for a long time you should check the Event Recorder whether it lists a continuous series of switching operations. If this is the case then you should check the auxiliary contacts that are used for position indications. There might be a bad contact, or the corresponding Digital Input might be configured to a wrong voltage level. In either case there can be a chattering of the input signal,

Description	Information	Corrective Action
		which causes the protection device to be flooded with signals of switching operations.

3.4   Protection and Control

Description	Information	Corrective Action
After first start-up of the protective device there is a pending trip.	*Two red LEDs are illuminated at the front of the HMI. They indicate a trip and an alarm.*	With the factory default settings the protection relay is configured with an undervoltage protection. Adapt the settings of the undervoltage protection or remove this module from the device project settings (if you do not need it). If you have any problems with acknowledging the pending alarm, please refer to "The binary outputs or LEDs are in unexpected state".
The **switchgears cannot be operated by SCADA communication**.		Set the [Control / General Settings] »*Switching Authority*« of the device to either "Remote" or "Local and Remote".
Problem with current and voltage measurement.	*The measured values of current and voltage show a big fluctuation.*	Adjust [Field Para / General Settings] »*f*« to the connected grid frequency (50 Hz or 60 Hz).
The **trip command is kept in latched state**.	*A latched trip command has been reconfigured from latched to unlatched.*	Only until Release 3.5: The status of the trip command must be acknowledged once, if it had already been pending before the reconfiguration. (As of Release 3.6, no action is required.) Independent of this, note that a latched trip command even »survives« a restart of the device.
Binary outputs do not react.	*The contacts of the binary outputs do not open or close. This can be checked by simulating a fault and checking the binary output contacts with measurement equipment.*	Check the following issues: • Acknowledge the binary outputs, if applicable. • Is the status of the binary output forced to a dedicated value? (The binary output can be overwritten for commissioning purpose, see menu branch [Service / Test (Prot inhibit)].) • Is the correct parameter set active (1…4)? • Is the required protection function active? • Is overall protection active? • Are the field parameters set correctly (CT ratio etc.)? • Are the protection parameters set correctly (trip value, trip time)? • Is the assigned protection function blocked? • Is the protection function's trip signal routed to the Trip-Manager of the correct switchgear? • Is the trip signal of the switchgear routed to the correct binary output?

Description	Information	Corrective Action
		• Is the wiring correct?
Failure of control *from local or remote.*	*Neither local nor remote switch commands succeed.*	Check the following issues: • Is the switch command blocked? • Is the wiring correct? • Do you have switching authority? Check the value of switching authority ("None", "Local", "Remote", "Local and Remote"). • Is switching blocked by the synchro-check?

3.5   Communication

Description	Information	Corrective Action
Failure of time synchronization.		Check the following issues: • Is the correct protocol for time synchronization selected ([Device Para / Time / TimeSync / TimeSync] *»TimeSync«*)? • Is the timezone set correctly ([Device Para / Time / Timezone] *»Time Zones«*)? • Open the status page of the used protocol. Check, if the module works correctly. • IRIG-B: Is the correct type (IRIGB-00x) selected ([Device Para / Time / TimeSync / IRIG-B] *»IRIG-B00X«*)? • SNTP: See next entry.
Failure of SNTP time synchronization.	*There is no SNTP signal for more than 120 seconds, the SNTP status changes from "active" to "inactive" and an entry in the Event Recorder is set.*	The SNTP functionality can be checked in the [Operation / Status Display / TimeSync / SNTP] menu. If the SNTP status is not "active", please proceed as follows: • Check if the wiring is correct (Ethernet-cable connected). • Check if a valid IP address is set in the device at [Device Para / TCP/IP / TCP/IP config]. • Check if the IP address of a valid NTP Server is set ([Device Para / Time / TimeSync / SNTP] *»IP Byte1«…»IP Byte4«*)? • Check if SNTP is used for time synchronization at [Device Para / Time / TimeSync / TimeSync]. • Check if the Ethernet connection is active: [Device Para / TCP/IP / TCP/IP config] *»Link«* = "Up"?. • Check if the SNTP server as well as the protection device answers to a Ping. • Check if the SNTP server is up and working.
Failure of the TCP/IP connection		Check the following issues with your local IT: • Does the device answer a "ping" request? • If the device and the PC are part of different subnets, the gateway and subnet mask have to be set correctly within the device ([Device Para / TCP/IP / TCP/IP config] *»TCP/IP config«*).

Description	Information	Corrective Action
		• Is network communication blocked by a firewall?
TCP/IP connection between Smart view and protection device cannot be established.	In rare cases it is not possible to establish a TCP/IP connection to port 52152 (although no firewall blocks this port). This has been observed only in rare cases with Windows 7 and Windows 8.x systems that are not fully upgraded.	This type of connection problem can only be solved by upgrading the Windows operating system, i. e. installing all available service packs and upgrade packages that are available from Microsoft.
The **USB COM port is not visible** on the PC.	The USB port (e. g. COM 5) is not visible in Smart view.	Open the Device Manager of the Windows PC, and check the entries below "Connections (COM & LPT)". • If the protection device is listed as a generic "Serial USB Device (COM n)" [Windows 10], or as an "Unknown Device" [Windows 7] then the USB driver has not been properly installed during the installation of Smart view. (Re-)Install the USB driver that comes with the Smart view setup. (Driver installations require Administrator privileges.) A connected HighPROTEC device must be listed as "… HighPROTEC USB (COM n)" in the Device Manager.
	It is not possible to connect Smart view, the Field Device Installer or some other application to the device via USB. The corresponding USB port (e. g. COM 5) is not visible in the application.	Check the following issues: • Smart view: Is a sufficiently up-to-date version installed (4.40 or higher)? • Plug off the USB cable from the protective device and plug it in again. After 10 seconds try again to connect Smart view (or Field Device Installer) to the relay. • Restart your PC.
The **USB COM port is visible, but no connection** is possible.	It is not possible to communicate with Smart view to the relay via USB. The corresponding USB port (e. g. COM 5) is available and has been selected correctly.	Check the following issues: • Is Smart view access via USB enabled on the device? Check the settings at [Device Para / Security / Communication]. • Is the USB port of the PC still occupied by another application (or program)? Close those applications. • Is the protective device started up completely?
	The corresponding USB port (e. g. COM 5) is available and has been selected correctly, but the Windows operating system reports an "Error 720" as soon as Smart view tries to talk to the protection device over USB.	The communication between Smart view and a HighPROTEC device uses the IPv4 internet protocol, wrapped into a PPP ("Point-to-Point Protocol") serial connection.

Description	Information	Corrective Action
		Therefore make sure that your Windows PC supports the IPv4 internet protocol. (The connection is not possible if only IPv6 is available on the Windows PC.)
*For older protective devices with RS232: Smart view does **not connect via RS232**.*	*It is not possible to communicate with Smart view from a PC to the device via RS232.*	Use *Smart view* version 4.40 or higher. If your PC does not have a serial port, you need a USB-to-serial-adapter that has been approved by SEG. (See *Smart view* manual.) This has to be installed correctly. Verify that your cable is a zero-modem cable (please refer to the *Smart view* manual). A simple serial cable does not have any flow control lines. A connection is only possible with a zero-modem cable.
*Smart view reports "**Internal TLS Connection Error.**"*	*Smart view starts to establish a connection to the device, but the key exchange procedure is not successful and results in the error message "Internal TLS Connection Error".*	Check the date and time settings of your device by using the Panel HMI. Make sure that the date is not before the year 2018.
*Smart view **cannot connect to the device** although this has been possible before using the same PC.*	*A connection between Smart view and device has been possible before using the same PC. Now it is no longer possible to connect to the device.*	Check the following issues: • Are the connection settings of *Smart view* correct? (Check at menu [Settings / Device Connection…].) In case of Ethernet (TCP) connection: Is the correct IP address selected? • Is *Smart view* access enabled on the device? Check the settings at [Device Para / Security / Communication]. • Check the wiring between PC and device. • In case of Ethernet (TCP) connections: Is the TCP/IP connection working? Refer to Failure of the TCP/IP connection. • Wait for 15 minutes and then try again to connect to the device. • Restart your PC and then try again to connect to the device.
***No communication (data transfer)** with Smart view possible, even though a connection has been established.*	*Required TCP/IP ports are blocked by a firewall.*	Make sure that no TCP/IP port in the range 52152 … 52163 is blocked.
*Line Differential protection devices: Smart view **remote connection not possible**.*	*Required TCP/IP ports are blocked by a firewall, or the remote connection is disabled by the device settings.*	Check the following issues: • Check the settings of your firewall. Make sure that no TCP/IP port in the range 52152 … 52163 is blocked.

Description	Information	Corrective Action
		• Check the settings of your **local** device: [Protection Para / Global Prot Para / Prot-Transfer / ProtCom] »*Use remote access*« has to be set to "active". • Check the settings of your **remote** device: Is *Smart view* access via ProtCom enabled on the device? [Device Para / Security / Communication] »*Sm. view via ProtCom*« has to be set to "active".

Line Differential protection devices: **Protection Communication is not working**.	*The state of* [Operation / Status Display / Prot-Transfer / ProtCom / State] »*Comm.Ok*« *is* **0**.	Check [Operation / Status Display / Prot-Transfer / ProtCom / State] »Communication«:
		
		 • "Err (no RX)" or "Err (no TX)"
		    ○ Check the wiring.
		    ○ Verify that fiber optic line is connected to the correct fiber optic port.
		
		 • "Err (corrupt data)"
		    ○ The device is connected to a non-compatible (i. e. non-Troubleshooting_HPT) device.
		
		 • "Err (incomp. IDs)"
		    ○ The device is connected to the wrong partner device, or
		    ○ check the setting value of [Protection Para / Global Prot Para / Prot-Transfer / ProtCom] »*Pair ID*«.
		
		 • "Err (incomp. Freq)"
		    ○ The devices are configured to different nominal frequencies.
		
		 • "Err (incomp. FW)"
		    ○ The devices use different firmware versions. Update the firmware.
		
		 • "Err (incomp. Sync 1)" or "Err (incomp. Sync 2)"
		    ○ Fiber optic not plugged in correctly.
		    ○ Fiber optic lines are too long.
		    ○ Fiber optic lines are damaged.
		    ○ Fiber optic connectors are damaged.
		    ○ You can do a test of the fiber optic port (see Loopback Test).
		
		 • "Ok (some errors)"
		    ○ Some errors occurred during normal protection communication. Check the value of [Operation / Status Display / Prot-Transfer / ProtCom / State] »24h Err Cr«.

Description	Information	Corrective Action

		Errors may occur when plugging in or out the connection line. The counter can be reset via [Operation / Reset] »Res all Cr/Err«.
		
		You can adjust the warning level under [Protection Para / Global Prot Para / Prot-Transfer / ProtCom] »24h Err WarnLev«.
		
		• "Eth.Switch det."
		  ◦ Devices are connected via a switch. Proper operation can only be guaranteed for direct device connection. Please adjust.
		• "Ok (stable)"
		  ◦ Protection communication is running stable.

*Line Differential protection devices: **Protection Communication is not working** as expected.*	*Protection Communication is working, but not correctly. The state of* [Operation / Status Display / Prot-Transfer / ProtCom / State] *»Comm.Ok« is **1**.*	If [Operation / Status Display / Prot-Transfer / ProtCom / Advanced States] »Operating Mode« is "Loopback", you have a loopback connection between RX and TX of your device. Please adjust the wiring.

3.6   Recorder

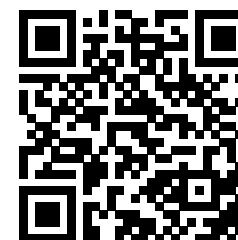| Description	Information	Corrective Action
The **Event Recorder is permanently logging new events**.	The Event Recorder ([Operation / Recorders / Event rec] »Event rec«) does permanently show new events. To observe this phenomenon in Smart view, please execute a "refresh" (»F5« or »Ctrl«+»F5«).	Proceed as follows: • Check the Event Recorder to see which protection function is creating the events. • Check the settings of this protection function. Adapt them, if necessary. Example: Protection function »df/dt« is configured too sensitive and is creating alarms with high frequency. Change the settings of this function.
The **Disturbance Recorder is permanently logging new records**.	The Disturbance Recorder ([Operation / Recorders / Disturb rec] »Disturb rec«) shows a high number of created disturbance records. This number is growing constantly over time. To observe this phenomenon in Smart view, please execute a "refresh" (»F5« or »Ctrl«+»F5«).	Check the following issues: • Check at [Device Para / Recorders / Disturb rec] which events (e. g. Protection Alarm) are configured to trigger the Disturbance Recorder. • Check within the Event Recorder ([Operation / Recorders / Event rec] »Event rec«), which protection function creates the trigger. • Check the settings of this protection function. Adapt them, if necessary. Example: Protection function »df/dt« is configured too sensitive and is creating alarms with high frequency. Change the settings of this function. Alternatively you can also change the trigger source of the Disturbance Recorder. But in general, this is less advisable.

docs.SEGelectronics.de/hpt-2-tsg

TROUBLESHOOTING GUIDE | **HighPROTEC**