SMART CABLE GUARD

Smart Cable Guard 2.0 Installation manual

Document information

Document title:	Smart Cable Guard 2.0 Installation manual	Energy Systems DNV Netherlands B.V.
Date of issue:	2026-03-10	Utrechtseweg 310-B50
Document No.:	SCG-129	6812 AR Arnhem
Revision No.:	rev. 9	The Netherlands
SCG department	☒ Product Management ☐ Insights ☐ Operations ☐ Sales and Marketing	Tel: +31 26 356 9111 Registered Arnhem 09006404

SCG review classification:	☒ E	☐ EC	☐ I	☐ -T	☐ X
Document classification	☐ Open	☒ DNV Restricted	☐ DNV Confidential* *(*list persons)*	☐ DNV Secret* *(*list persons)*	

Keywords: Installation manual, SCG 2.0, Hardware

Rev. No.	Date	Reason for Issue	Prepared by	Verified by	Approved by
0	2916-09-20	Initial version	PW	PW	PW
1	2016-11-04	Updates	PW	PW	PW
2	2016-12-08	Updates	PW	PW	PW
3	2017-05-01	Updates	PW	PW	PW
4	2018-10-30	Updates	PW	PW	PW
5	2020-05-01	Updates	PW	PW	PW
6	2022-10-18	Updates	PW	PW	PW
7	2026-01-21	Refresh and fixed broken links	MM	PW	PW
8	2026-01-29	Note added with the sim card installation	MM	PW	PW
9	2026-02-04	Update sim card pictures and restructuring	MM	PW	PW
10	2026-03-10	Bookmark missing	MM	PW	PW

CONTENTS

1 INTRODUCTION 2
1.1 Intended use of equipment 2
1.2 Safety Symbols and Terms 2
1.3 General attention points 2
1.4 Contacting DNV 3

2 REQUIRED MATERIALS FOR INSTALLATION 4
2.1 Control Unit (CU) overview 5
2.2 Sensor Unit (SU) overview 7

3 INSTALLATION PROCEDURE 8
3.1 Tools and mounting hardware 8
3.2 Preparation before installation 8
3.3 Installing the SIM card 8
3.4 Installation in the field 11

4 PHYSICAL INSTALLATION 13
4.1 Installing the Control Unit 13
4.2 Connecting the wired LAN connection 14
4.3 Installing the Sensor Unit 14

5 CONFIGURATION 16
5.1 Connecting a laptop to the Control Unit 16
5.2 Identification information 17
5.3 Network Settings 18
5.3.1 Configuring the mobile data connection 18
5.3.2 Configuring the wired LAN connection 19
5.4 Sensor Unit settings 20

6 MAINTENANCE 22
6.1 Required maintenance actions 22
6.2 Cleaning 22
6.3 Replacing fuses 22
6.4 Firmware updates 23

7 TROUBLESHOOTING 26
7.1 No power supply to the system 26
7.2 The system is trying to communicate with the server 26
7.3 The auto-sync doesn’t detect the system at the other side of the cable circuit 27
7.4 Internal error – continuous red LED 28
7.5 SCG Control Unit Connector program shows the Control Unit, but it won’t open in the browser 28

APPENDIX A: PRODUCT SPECIFICATIONS 29

APPENDIX B: OVERVIEW OF STANDARDS 30

APPENDIX C: NETWORKING BETWEEN LAPTOP AND CONTROL UNIT 33

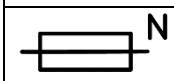
1 INTRODUCTION

1.1 Intended use of equipment

Smart Cable Guard is an advanced tool that accurately locates faults in any kind of medium-voltage (MV) cable network and provides information of weaknesses in MV cables. The Sensor Units are installed around the cable or earth lead of the cable circuit. Each Sensor Unit is connected to a Control Unit, which provides possibility to configure the system and performs analysis of measured signals and communicates the results to the server.

1.2 Safety Symbols and Terms

The following symbols and terms appear on the equipment or in this manual. The symbols and terms alert you to important safety considerations.

	This symbol warns of a potential risk of electrical shock
	This symbol is used to warn the user to be cautious and to refer to this manual for more instructions.
	This symbol is used to denote a protective earth (ground) connection.
	This symbol is used to denote a functional earth (ground) connection
	This symbol is used to indicate that the neutral is fused as well.
Attention	The **Attention** term indicates a potential hazard. It calls attention to a potential procedure, practice or condition which, if not followed, could possibly cause damage to the equipment, or could possibly cause bodily harm or death. If an **Attention** is indicated, do not proceed until its conditions are fully understood and met.

1.3 General attention points

Attention

Do not use the equipment in a manner not specified by the manufacturer. Any incorrect use of the equipment could possibly result in damage to the equipment, bodily harm or death.

Attention

The Control Unit and Sensor Unit must be handled with care. Do not bump or drop any part of the Control Unit or Sensor Unit.

Attention

Do not replace the mains power cable by any cable other than specified by the manufacturer.

Attention

Use the Sensor Unit only with the supplied AC/DC adapter.

Attention

Information in this manual is subject to change without notice.

1.4 Contacting DNV

For general information regarding Smart Cable Guard, visit www.dnv.com/scg

For documentation regarding Smart Cable Guard, visit www.dnv.com/scg2downloads.

For questions during installation or application of Smart Cable Guard, send email to scg-global@dnv.com.

2 REQUIRED MATERIALS FOR INSTALLATION

The Smart Cable Guard hardware works in pairs, one Control Unit and Sensor Unit must be installed at the start of the monitored cable, and one Control Unit and one Sensor Unit must be installed at the end of the monitored cable. Each Control Unit can be connected to up to 3 Sensors Units, allowing it to monitor 3 different cables.

To install one set of Smart Cable Guard 2 the following materials are necessary:

- **Smart Cable Guard 2 devices:**



1 Control Unit



1 to 3 Sensor Units

- **Cables and accessories:**



Grounding wires and terminals for all devices



Micro SIM card



Cable cord with a C13 connector for Control Unit



1 to 3 AC/DC adapter for the Sensor Unit + Cable cord



1 to 3 Fiber optic cable with SC duplex to SC duplex connectors



Antenna



Ethernet cable with RJ45 connectors

2.1 Control Unit (CU) overview

An overview of the Control Unit and all its parts are shown in Figure 1.



Figure 1 Overview of the Control Unit

The individual parts shown in Figure 1 are:

1. Top cover
2. Safety earth connection (size M6)
3. Mains connection socket (100-230 Vac), with slots for two fuses
4. Product identification label
5. Antenna connector for mobile data connection
6. Auto-sync button of Sensor Unit port 3.
7. Status indicator of Sensor Unit port 3. This indicator has the following patterns:

LED indication	Status
Off	No connection with the Sensor Unit, or the Sensor Unit has no supply voltage
Green blinking	Sensor Unit is connected, but it not in sync with its partner at the other end of the cable circuit
Green continuously on	Sensor Unit is connected and in sync with its partner at the other end of the cable circuit
Green/red blinking	Auto-sync procedure is in progress (please wait)

Green/orange blinking	Sensor Unit firmware is being updated. Do not disconnect or power off the Sensor Unit while this is happening. The Sensor Unit firmware update lasts a maximum of 1 minute.
Orange/red blinking	System is starting up (all LEDs are blinking orange/red)
Red continuously on	Sensor Unit reports an internal error

8. Optical fibre connector of Sensor Unit port 3.
9. Wired local-area-network (LAN) connection for configuration via laptop and optionally for communication with server
10. Status indicator for server communication. This indicator has the follow patterns:

LED indication	**Status**
Off	The Control Unit is switched off; it has no mains connection
Green blinking	Trying to connect to the server
Green continuously on	Successful connection with the server
Orange/red blinking	System is starting up (all LEDs are blinking orange/red)
Red continuously on	Control Unit encountered an internal error (e.g. an incorrect PIN-code)

11. Reset button, to perform a soft or hard reset of the Control Unit:

Function	**Action**	**Description**
Soft reset	Short press (<5 seconds)	Gracefully shuts down the firmware in the Control Unit and reboots it afterwards.
Hard reset	Press and hold the reset button for 15 seconds	**There is a small chance that files on the Control Unit become corrupt when a hard reset is performed. Therefore, use the hard reset only as the last resort if the soft reset doesn't work**.

12. Mounting brackets

2.2 Sensor Unit (SU) overview

An overview of the Sensor Unit and all its part is shown in Figure 2.



Figure 2 Overview of the Sensor Unit

The individual parts shown in the figure are:

1. Sensor Unit aperture with insulation
2. Functional earth connection (size M6)
3. Optical fibre connector
4. DC power supply connector (5 Vdc)
5. Product identification label
6. Two draw bolts (size M5) to hold the two halves of the Sensor Unit together. The two halves are separable so that it can be clamped around the cable circuit.



3 INSTALLATION PROCEDURE

This chapter describes the steps required to install a complete Smart Cable Guard system, consisting of two Control Units and two Sensor Units.

3.1 Tools and mounting hardware

The tools and hardware necessary for the installation are listed below:



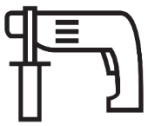
Mounting hardware: nuts and bolts



M6 wrench for grounding bolts



Phillips-head screwdriver



Tools to prepare the mounting surface (e.g. drill)

3.2 Preparation before installation

1. Configure both Control Units. For each unit:
    a. Install the SIM-card, if required, and configure the communication settings (see Section 3.3 and Section 5.3.1).
    b. Check the server status indication light (number 10 in Figure 1) to determine whether the system has a connection with the server. A continuous green light indicates a successful server connection.
    c. Enter the identification information about the (RMU) or station where this system will be installed (see section 5.2)
    d. Enter the Sensor Unit settings (see section 5.4)
        i. One Sensor Unit must be configured as primary, the other Sensor Unit as secondary
        ii. Both primary and secondary Sensor Unit must be configured to use the same channel number
2. If other measurement systems are installed nearby in the same network, for example in the same feeder, then the channel number must be different from those systems.

3.3 Installing the SIM card

Follow the instructions in this section to use the mobile data connection for communication with the server and to install the SIM Card in the Control Unit.

Tip

To prevent any delays during installation, it is recommended to configure and test the mobile data connection before installing the system in the field.

1. Disconnect the power cable from the Control Unit

Attention

To avoid electrical shock, disconnect the power cable from the Control Unit before opening the top cover.

2. Remove the the top cover of the Control Unit:



Figure 3 The Control Unit with to top cover removed

Attention

Directly after disconnecting the power cable the internal UPS is still charged to a voltage of 6 volts. To prevent permanent damage to the device, prevent short-circuiting any internal parts of the Control Unit.

3. Wait until the UPS is completely discharge before proceeding to the next step. This can be checked by seeing the green LED light on the modem board, which should be off.

   NB: The pictures below the SIM-card slot slide open to the right, but your version may slide upward.



OR



Figure 4 Green LED on modem board indicating that modem is still powered

4. Locate the SIM card slot:

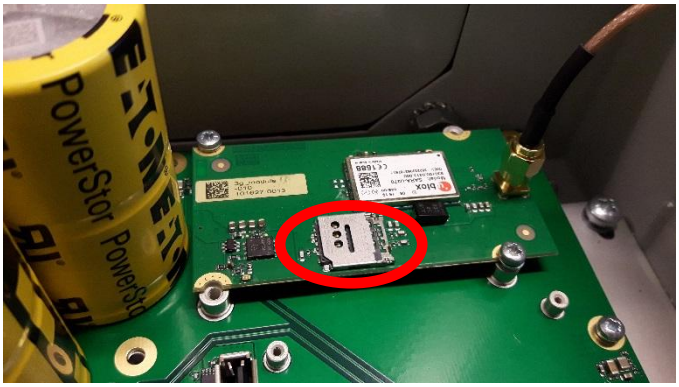


Figure 5 The location of the SIM card slot

5. Open the SIM card slot by sliding it to the side and tilting it open:



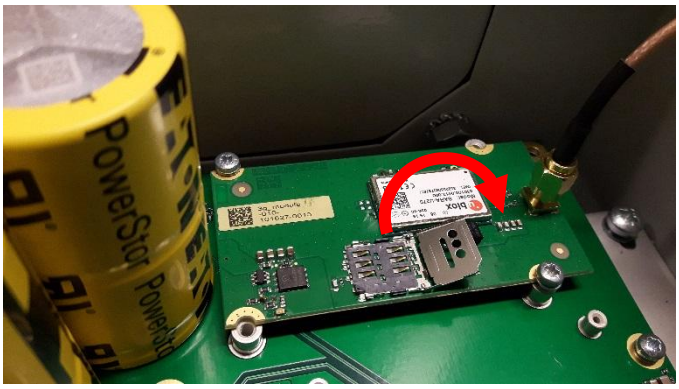


Figure 6 The opening of the SIM card slot

6. Insert the SIM card.

   Note: corner of the SIM card with diagonal cut is on the bottom-left in the picture (indicated by the red arrow)



Figure 7 The SIM card inserted

7. Close the SIM card slot



Figure 8 Closing of the SIM card slot

8. Close the top cover of the Control Unit

   Attention

   Ensure that the bolts are inserted and fixed in the right way so no water can enter via the top cover of the Control Unit

3.4 Installation in the field

1. Go to the first RMU or station and install the Control Unit and Sensor Unit configured as ***primary***. In order the use the auto-sync feature the ***primary*** must be installed first.

   a. Check the server status indication light (number 10 in Figure 1 on page 5) to determine whether the system has a connection with the server.
   A continuous green light indicates a successful server connection.

b. Check the Sensor Unit status light (number 7 in Figure 1 on page 5) to determine whether the Control Unit sees the Sensor Unit.
A green blinking light indicates that the Control Unit has a connection with the Sensor Unit.

2. Go the RMU or station at the other end of the cable circuit and install the Control Unit and Sensor Unit configure as ***secondary***. In order the use the auto-sync feature the ***secondary*** must be installed last.

   a. Check the server status indication light (number 10 in Figure 1 on page 5) to determine whether the system has a connection with the server.
   A continuous green light indicates a successful server connection.

   b. Check the Sensor Unit status light (number 7 in Figure 1 on page 5) to determine whether the Control Unit communicates with the Sensor Unit.
   A green blinking light indicates that the Control Unit has connection with the Sensor Unit.

3. Start the auto-sync procedure by pressing the auto-sync button (number 6 in Figure 1 on page 5) of the ***secondary*** Sensor Unit.

   a. The auto-sync procedure starts. The Sensor Unit status indicator starts blinking green and red to indicate that the auto-sync procedure is running. This will take a few minutes.

   b. When the auto-sync procedure is finished, a continuous green light indicates that the secondary Sensor Unit has detected the primary Sensor Unit at the other side of the cable circuit.
   If, after the auto-sync procedure, the light goes back to blinking green light, this indicates that the system could not find the primary at the other side of the cable circuit. See section 7.3 for troubleshooting steps.

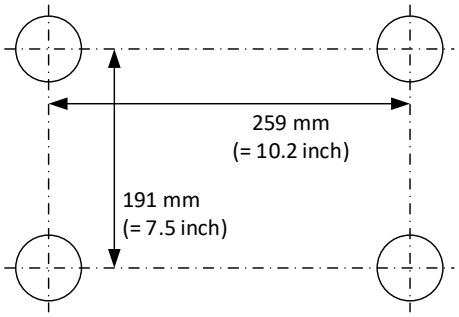
4. Send the installation form with circuit information to the DNV operator (scg-global@dnv.com) to perform a fine-tuning of the synchronization settings and enter the cable circuit on the Smart Cable Guard website (https://scg.dnv.com/).

4 PHYSICAL INSTALLATION

This section of the manual describes the methods of physical installation of the Smart Cable Guard system in the cable circuit.

4.1 Installing the Control Unit

1. Before installation, make sure that the power cable is disconnected from the Control Unit.
2. The Control Unit has four mounting brackets, one on each corner. The Control Unit must be mounted on a vertical wall or rack using the following steps:
    a. Identify a suitable vertical surface (for example a wall or rack) for mounting the Control Unit. The surface must be sufficiently strong to support the Control Unit.
    b. Drill four holes (or otherwise prepare suitable fixation points) for the four mounting brackets of the Control Units. These holes must have distances as indicated in the figure below:



    c. Use four bolts to mount the four mounting brackets into the drilled holes. The front panel (with the connectors) of the Control Unit must be facing down.

Attention

The Control Unit must be mounted vertically with the connectors facing down to avoid ingress of dust and water.

3. Connect the safety earth of the Control Unit to the earth rail of the station with a copper wire of at least 2.5 mm^2.

Attention

To avoid the risk of electrical shock, connect the safety earth of the Control Unit to the earth rail of the station.

4. If the Control Unit is configured to use the mobile data connection for server communication, then connect the antenna to the Control Unit. Position the antenna in a manner that it is not in contact with other metal parts in the station.
5. If the Control Unit is configured to use the wired LAN connection for server communication, then use a category (cat.) 5 (or better) network cable to connect the Control Unit to an Ethernet wall socket with network access.
6. Connect the power cable to the Control Unit and plug it in a wall socket.

The Control Unit has the following options for communication with the server:

- Wired LAN connection, see section 4.2.
- Mobile data connection using the modem inside the Control Unit, see section 3.3.

Choose one of these options for communication between the server and the Control Unit.

4.2 Connecting the wired LAN connection

Use the following steps to connect the Control Unit to a wired LAN connection.

1. Locate the LAN port on the Control Unit. In Figure 1 the LAN port labelled with number 9.
2. Insert one end of network cable[1] in the LAN port.

Insert the other end of the network cable in an Ethernet wall socket or switch. The wall socket must provide access to the Smart Cable Guard server. Usually, this connection goes via the internet.
Please contact your local network administrator for assistance in selecting the correct LAN wall socket or switch.

4.3 Installing the Sensor Unit

1. Before installation, make sure that the power cable is disconnected from the Sensor Unit.
2. Use Figure 9 on page 15 to identify the correct location for installing the Sensor Unit.
3. The Sensor Unit consists of two separate parts so that it can be clamped around a cable or earth lead. Use the two draw bolts (6a and 6b in Figure 2) to separate the two halves.
4. Clamp the two Sensor Unit halves around the cable or earth lead at the correct location.
5. Use a torque wrench to tighten the two bolts with a torque of 2.5 Nm.
6. Connect the earth connection of the Sensor Unit to the earth rail of the station with a copper wire of at least 2.5 mm^2.
7. Connect the optical fibre cable between the Sensor Unit and the Control Unit.
8. Connect the external DC power supply to the Sensor Unit and plug it in the wall socket. The Sensor Unit must be installed either around the earth connection, or around the cable itself. When installing around the cable, make sure that the position of the Sensor Unit relative to the cable earth connection is correct. For optimal noise reduction, make sure that the casing of the Sensor Unit does not touch other earthed parts in the station.

[1] The network cable must be a Category 5 or 6 Ethernet cable. Most standard network cables are one of these types.

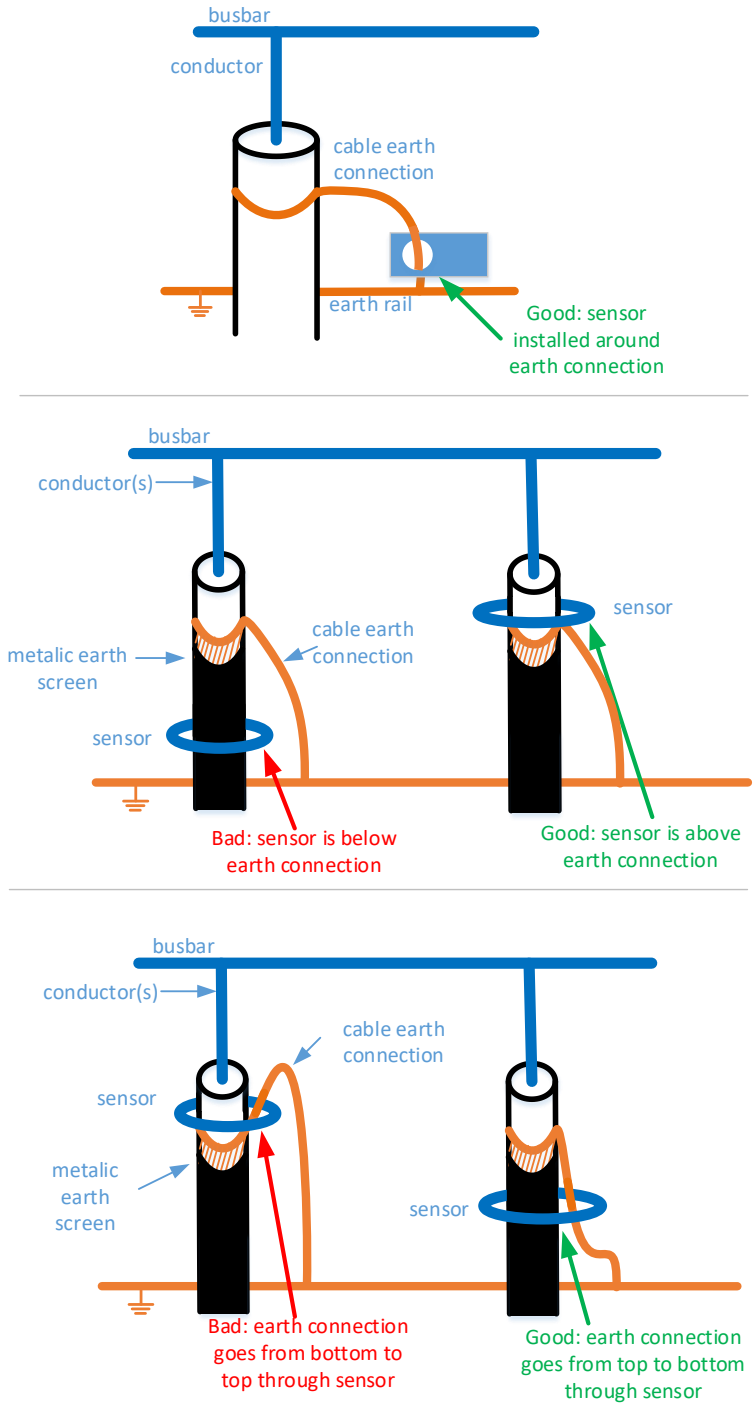


Figure 9 Sensor Unit installation locations.

5 CONFIGURATION

This section describes the configuration steps for the setup of the Smart Cable Guard system. For the setup, a laptop computer with at least Windows 7 and the latest versions of Edge, Firefox or Chrome are required.

Note that the Internet protocol TCP/IP of the used network adapter, the following options have been selected: "Obtain an IP address automatically" and "Automatic private IP address". These are the Windows default options. If not, please contact your local network administrator.

5.1 Connecting a laptop to the Control Unit

Use the following steps to connect a laptop to the Control Unit using a network cable:

1. Locate the LAN port on the Control Unit. In Figure 1, the LAN port labelled with number 9.
2. Disable the Wi-Fi connection for wireless networks on the laptop being used.
3. Insert one end of network cable[2] in the LAN port.
4. Insert the other end of the network cable in the network port of the laptop.

After the laptop is connected to the Control Unit, use the following configuration steps to access the configuration interface of the Control Unit:

1. Locate the SCG Control Unit Connector program on the laptop and start it. The program interface is shown in Figure 10.

   Note: the SCG Connector program (scg_connector_v1.0.exe) can be downloaded from https://www.dnv.com/scgsupport/.

2. When application is started, it automatically shows the connected Control Units. If not click “Restart discovery” to start searching for connected Control Units. The found Control Units, it will show up in the list. Select the Control Unit from the list are click “Open in browser”. The web browser will start with the configuration interface

[2] The network cable must be a Category 5 or 6 Ethernet cable. Most standard network cables are one of these types.

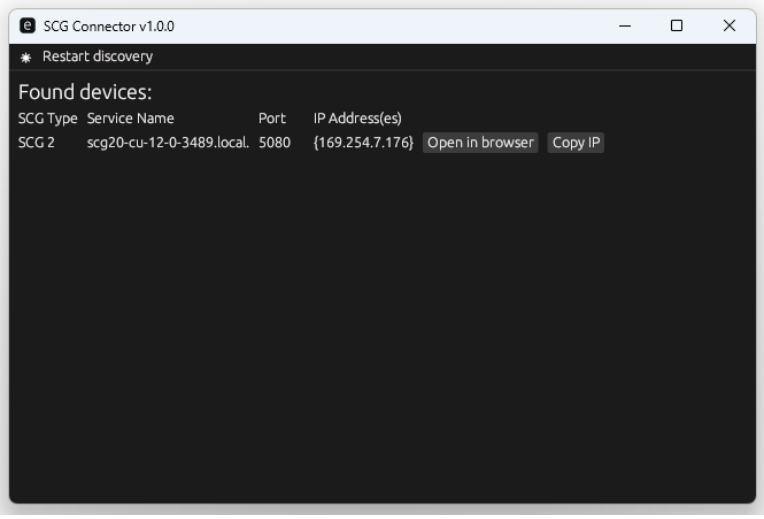


Figure 10 Interface of SCG Connector program

3. The Smart Cable Guard login screen is as shown in Figure 11.
4. To Log in, use Username: *scg* and Password: *scg*
5. Press Submit.

In case the scg_connector app does not find the Control Unit, then see for technical details on networking.



Figure 11 Login screen

5.2 Identification information

After logging in, the “Control Unit identification” tab is first displayed. An example is shown in Figure 12.

The following steps should be followed for entering information:

1. Check the Control Unit ID being displayed. This should be same as id on the Control Unit’s product label.
2. Fill in the information as asked.
3. Press Save.

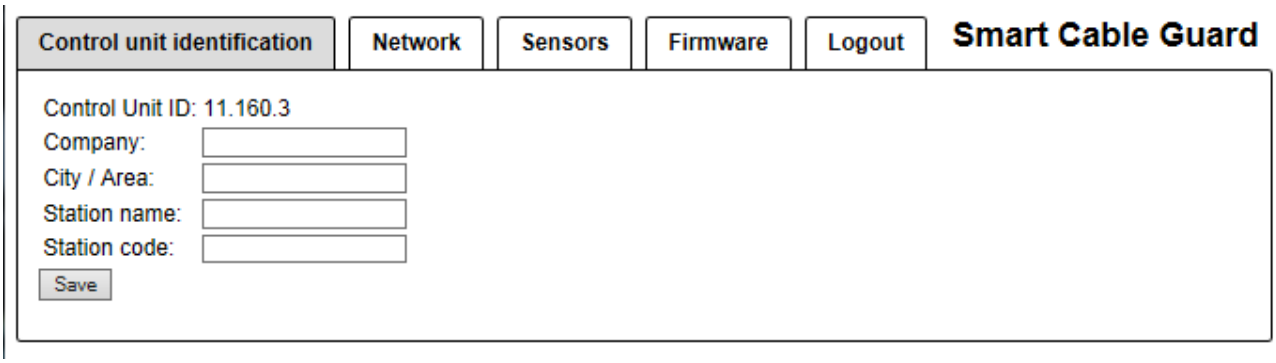


Figure 12 Control Unit identification

5.3 Network Settings

After Control Unit identification is complete, the next step is the network settings. It is important to decide whether a mobile data (3G/4G) or a LAN connection will be used for the communication between the system and the server before making any changes to this setting.

5.3.1 Configuring the mobile data connection

Installation of the sim card required for mobile data connection is described in section 3.3.

To configure the system using a mobile data connection, the following steps are used:

To get the Control Unit communicating via the mobile network, the network interface must be selected as “Cellular” (See

Figure 13).

Enter the network settings of the service provider and the PIN code of the SIM card under the “Mobile network settings” section (see red box in

Figure 13).

1. Choose the correct “Mobile network profile”. In most countries this will be “Standard Europe (100)”, but in some cases (USA and China for instance) a different profile is needed. See Figure 14 for all the options.

   For a complete overview of the LTE bands used worldwide, please visit this Wikipedia link: https://en.wikipedia.org/wiki/LTE_frequency_bands

   This step is only for SCG 2.0 CU 4G, when using SCG 2.0 CU 3G please skip to point 4.

2. The server address and port number should be requested from DNV. For most situations, the default values will be correct.
3. After entering the relevant information, click Save.
4. Perform a soft rest by pressing the reset button (identified as 11 on the Control Unit in Figure 1) for 1 second. It will take about 3 minutes to reboot the system.

To check if the Control Unit is communicating after performing soft reset, you can look on the Status LED for server communication on the Control Unit or log in again and look on the Network Status.

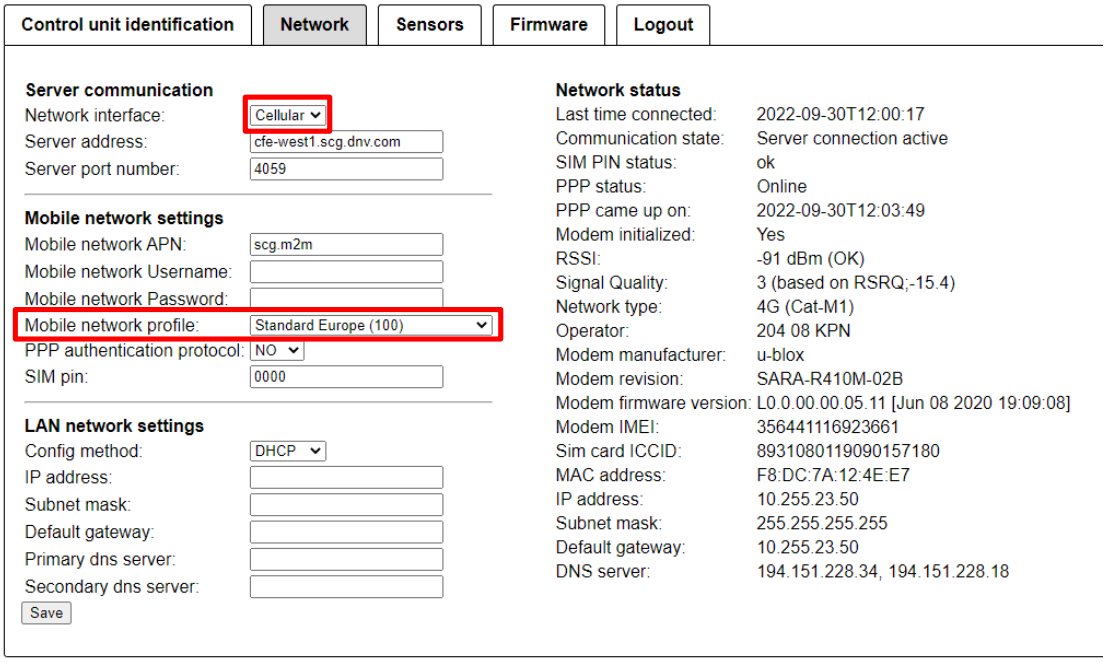


Figure 13 The Network settings and status from the mobile network, including Mobile Network Profile.

MNO	Version	System Selection	LTE Bands
AT&T	v 7.1	M1 only	2, 4, 5, 12
China Telecom	v 7.0	M1->NB1	3, 5, 8
Deutsche Telekom	v 7.0	M1->NB1	3, 8, 20
Sprint	v 7.0	M1 only	2, 4, 12, 25
Standard Europe	v 7.0	M1->NB1	3, 8, 20
Telstra	v 7.0	M1 only	3, 5, 8, 28
T-Mobile USA	v 7.0	NB1 only	2, 4, 5,12
TELUS	v 7.0	M1 only	2, 4, 5, 12
Verizon	v 7.0	M1 only	13
Vodafone	v 7.0	NB1->M1	3, 8, 20
SW default	N/A	M1->NB1	2, 3, 4, 5, 8, 12, 13, 18, 19, 20, and 25 as M1-only

Figure 14 The Mobile network profile options and LTE bands related to the options.

5.3.2 Configuring the wired LAN connection

Connection of the Control Unit to a LAN interface is described in section 4.2.

Follow the instructions in this section to use a wired LAN connection for communication with the server.

1. To get the Control Unit communicating via the LAN network, the network interface should be selected as “LAN” (see orange circle in Figure 15).
2. If DHCP is selected in the “LAN network settings” section’s drop-down menu, then appropriate information is filled by default (see red box in Figure 15).
3. The server address and port number should be requested from DNV. For most situations, the default values will be correct.
4. If “Static” is selected in the “LAN network settings” section’s drop-down menu, then enter the appropriate IP address and subnet mask values. This should be accordance to the local network provider.
5. After entering the relevant information, click Save.
6. Perform a soft rest by pressing the reset button (identified as 11 on the Control Unit in Figure 1) for 1 second. It will take about 3 minutes to reboot the system.

To check if the Control Unit is communicating after performing the soft reset, you can look at the Status LED for server communication on the Control Unit or log in again and look on the Network Status.

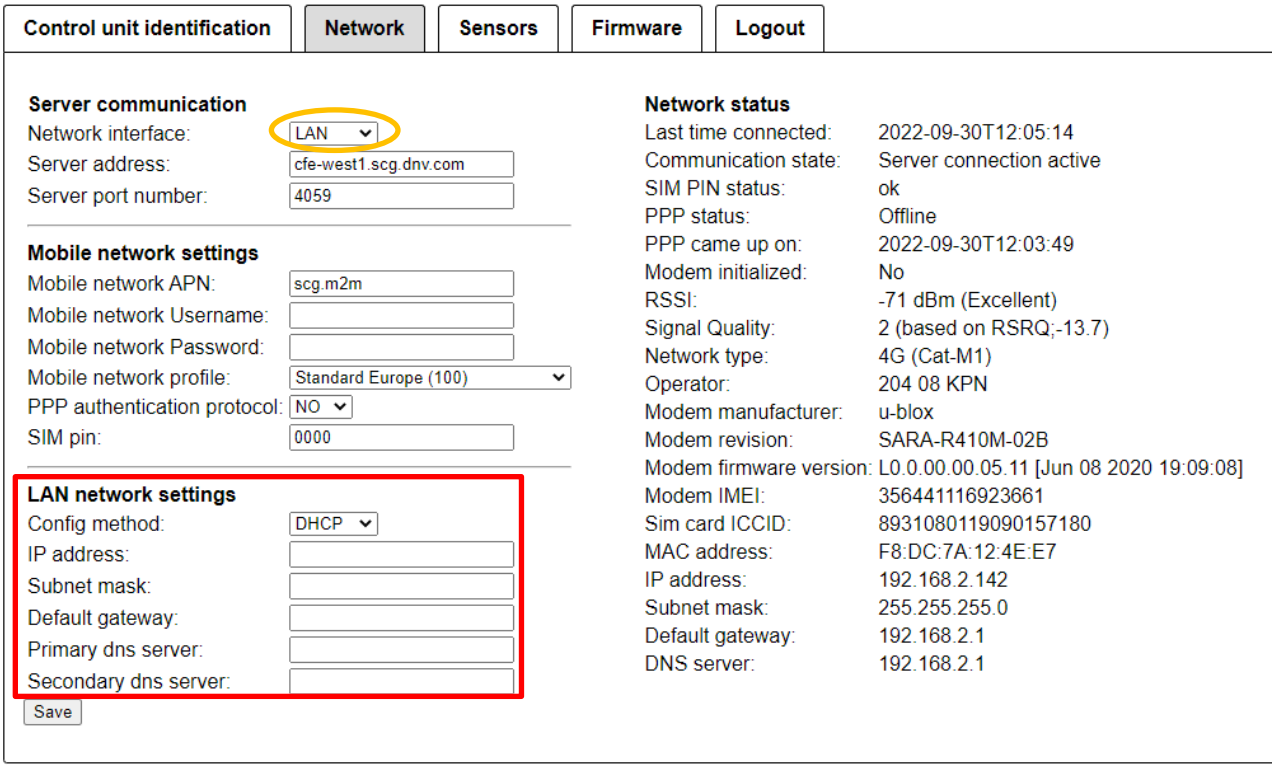


Figure 15 The Network settings and status from the LAN connection

5.4 Sensor Unit settings

After completion of the network settings, the next steps are the Sensor Unit settings. When this tab is selected, the connected Sensor Unit id numbers will be displayed in the respective connected port numbers, as shown in Figure 16. The mode of the active ports and the connected system can be selected to be as primary or secondary. After selecting this, choose a channel number from the drop-down menu. Ensure that the same channel number is used for a

monitoring system, i.e. the channel number should be same for the system at both ends of the cable circuit. After selecting an exclusive channel, press Submit.

Tip

Be aware of other Smart Cable Guard installations in the surrounding areas of the cable circuit to avoid a mixing of channels.



Figure 16 Sensor Unit settings

6 MAINTENANCE

6.1 Required maintenance actions

The following maintenance actions are required to ensure proper operation:

a) If a layer of dust settles on the equipment, then the dust must be removed to prevent overheating of the equipment. See section 6.2 for cleaning instructions.

b) If the fuses in the Control Unit are blown, they need to be replaced. See section 6.3 for instructions.

6.2 Cleaning

The general instructions to be followed while cleaning the equipment is presented below:

Attention

To avoid electrical shock, disconnect the power cable from the equipment before cleaning the equipment.

a) Disconnect the power cable from the Control Unit and wait for a minimum time of 45 minutes for the internal UPS to discharge completely.

b) Clean only the exterior of the equipment using soap and water on a damp, soft cloth.

c) Do not allow moisture to penetrate the equipment.

d) Do not submerge the equipment in water.

e) Do not use abrasive cleaners.

6.3 Replacing fuses

Use the following steps to replace the fuses in the Control Unit:

1. Disconnect the power cable from the Control Unit
2. Wait for the internal UPS to discharge completely for a minimum time of 45 minutes.

Attention

To avoid electrical shock, disconnect the power cable from the Control Unit before replacing the fuses.

3. On the Control Unit, locate the slot with the fuses. It is located below the mains connection socket:

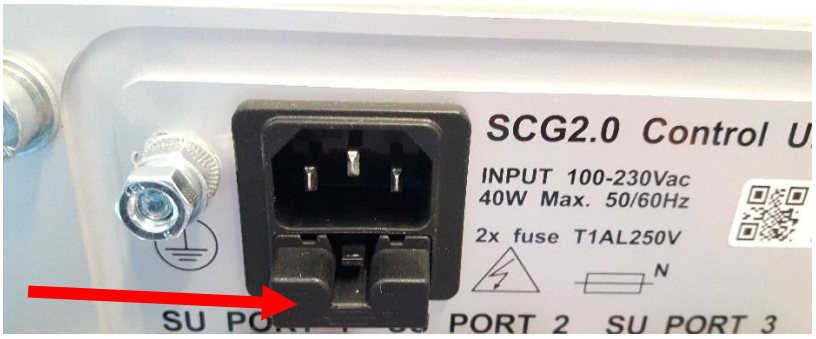


Figure 17 The fuse tray below the power connector.

4. Open the fuse slot:



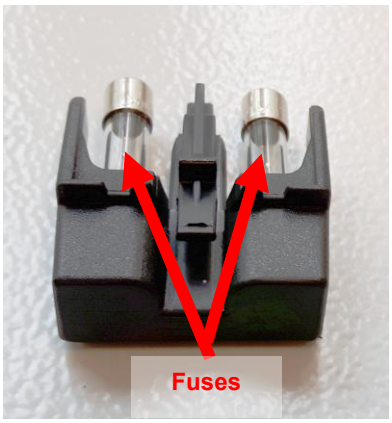


Figure 18 Fuse tray pulled out of the CU and fuses in fuse tray.

5. Replace the blown fuses with fuses of the follow type:

   1.6 A, 250 V, 5x20mm glass fuse, slow blow, little fuse 021301.6MXP

6. Close the fuse slot

6.4 Firmware updates

DNV will release firmware updates regularly. These contain bugfixes and/or new functionality. Most of the time these updates will be delivered Over-The-Air (OTA), via the mobile data connection. But in some cases, it can be possible that the Control Unit is not functioning correctly, and a local update is needed. The Control Unit can be updated using the following steps:

1. Connect your laptop to the Control Unit and login as described in section 5.1
2. Select the tab ‘Firmware’. One can find the current firmware version after ‘CU application version’
3. Click on ‘Choose file’

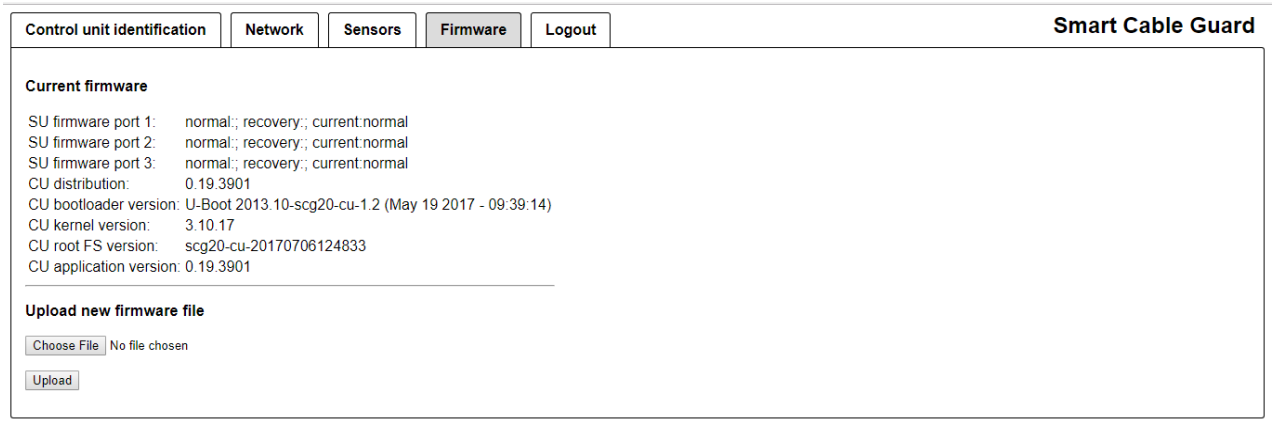


Figure 19 The firmware tab

4. Select the new firmware file (for example “appupdate_su_os_cu_1_3_4413.tgz.gpg”)

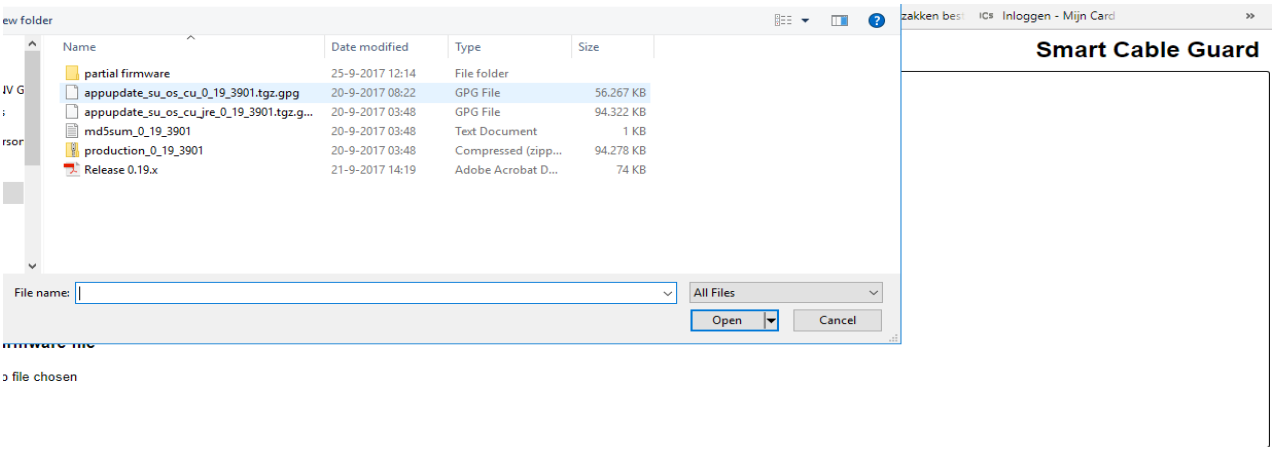


Figure 20 The explorer window that opens after clicking “Choose File”.

5. Click on ‘Upload’. The new firmware will be uploaded to the Control Unit. After a few seconds the message appears that the file is uploaded successfully.



Figure 21 After uploading a message will appear that the upload was successful.

6. The update process runs automatic. After the update the Control Unit will restart. During the restart the LED lights will blink red-orange for several seconds. The whole process will take about 3 minutes.
   It is important that during this process the Control Unit must not be reset or disconnected from the power supply!
   Note: it is possible that update process doesn't start, that means that the LED's never start blinking and the update is not applied. This problem can be caused by a setting in Internet Explorer. To solve:
   - ***In Internet Explorer, go to 'Internet Options' > 'Security tab' > '"Internet" or "Intranet"' > Click on 'Custom Level'. In the 'Security Settings' scroll down until you see "Include local directory path when uploading files to a server" and disable it. Click OK on Internet Options window and refresh the page.***
   - ***Another solution is to use another browser, such as Google Chrome.***
7. After the Control Unit is restarted, one can login again in the web interface.

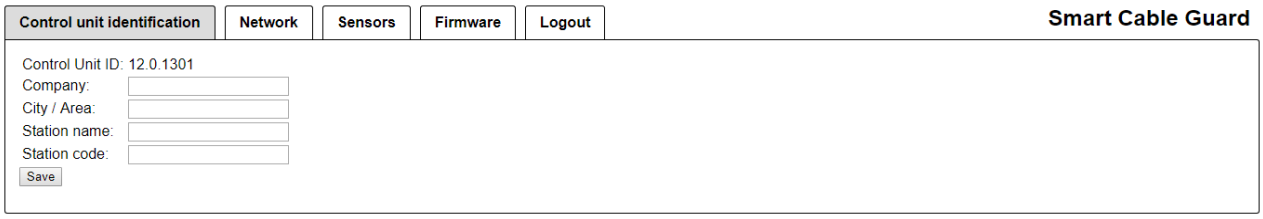


Figure 22 The Control Unit identification page.

After the firmware update succeeded. The Control Unit can be put in operation. All settings of the Control Unit have been saved during the update.

7 TROUBLESHOOTING

Most problems with the Smart Cable Guard installation can be diagnosed effectively with the help of the status indicator LEDs on the Control Unit. These LEDs indicate the status of the Sensor Unit and server communication, as presented in point 7 and point 10 in section 0 respectively.

An overview of the same is presented below:

LED STATUS	EXPLANATION	TROUBLESHOOTING STEPS
Control Unit status led: Off	No power supply	See section 7.1
Control Unit status led: Green blinking	1. System is trying to connect to the server	See section 7.2
Sensor Unit status led: Green blinking	2. Sensor Unit has no sync with partner at the other end of the cable circuit	See section 7.3
Server Unit status led: Red continuously on	Internal error	See sections 7.4

Other known problems are:

PROBLEM	TROUBLESHOOTING STEPS
SCG Control Unit Connector program shows the Control Unit, but it won't open in the browser	See section 7.5

7.1 No power supply to the system

An interruption to the power supply will not display the LED in the Control Unit or the Sensor Unit. Use the following steps to resolve this:

1. Wait 10 seconds to see if the LED turns on. When Control Unit is powered on after being off for a long time, it will take a few seconds to charge its internal UPS before the system starts up.
2. Check for a lose connection of the power supply cord to the Control Unit and Sensor Unit.
3. Check for an interruption in the grid power supply.
4. Check for damages on the lead of the power supply cord for the Control Unit and Sensor Unit.
5. Check if the fuse next to the mains connection socket is blown and requires a replacement. If yes, follow the steps listed in section 6.3.

7.2 The system is trying to communicate with the server

When the SCG system does not communicate with the server, it is usually due to the following issues:

1. SIM card errors

(a) The SIM card has not been mounted in the modem properly. Remove and replace the SIM card by following section 3.3.

(b) The SIM card settings are not entered or not entered correctly and saved. Recheck the settings from section 5.3.1.

(c) The SIM card subscription has expired or has been terminated otherwise. Ensure a valid subscription and connectivity for the SIM card.

2. Antenna Errors

    a. The antenna is not connected properly to the Control Unit and leads to no communication.

        i. Check if the antenna is installed on the system as per installation instructions in section 4.1, point 4 and is properly tightened to the magnetic base of the antenna.

    b. The signal of the antenna is being blocked due to the construction of the site where the cable circuit is installed or due to an external barrier or remote location of the transmission tower. Check the surroundings of the circuit-to-be-monitored and the cellular reception strength in the area with the station door closed.

    c. Perform a soft reset by a short press on the reset button next

3. Is LAN used instead of 3G: LAN connection errors

    a. The LAN connection is not working properly. Verify if the LAN cable is connected to a working internet connection.

7.3 The auto-sync doesn't detect the system at the other side of the cable circuit

The auto-sync on the system may not be able to detect the system at the other side of the cable circuit due to a loss of synchronisation between them: This can happen if:

1. The circuit is too long, or the attenuation of the cable is too high. Steps to be taken, if the cable circuit is too long being:

    a) Move installation to a shorter circuit

2. There is too much noise present on the cable. Such noise can, for example, be produced by a customer's installation. Installations with power electronics can cause problems. This noise can be higher than the amplitude of the sync pulse. Contact DNV for further assistance.

3. The circuit breaker is open. Check this connection.

4. The earth screen of the cable has not been earthed (properly) in cable circuit. Check this connection.

5. The Sensor Unit has not been installed at the correct location but around the cable below the last connection to earth.

The Sensor Unit must be installed either around the cable above the last connection to earth or around the last connection to earth itself. See section 4.3, **Error! Reference source not found.** for examples.

6. The Sensor Unit is installed in a short-circuited (earth) loop. This can happen if:

a) The metal inner ring of the Sensor Unit is not properly insulated and contacts the cable or earth wire around which the Sensor Unit is installed.

b) There is an “extra” earth connection in addition to the cable’s earth wire. Such as metal hooks, brackets or clamps that are electrically connected to the earth screen.

7. SCG has been installed on a large open installation.

8. Reactors have been connected in series with the guarded circuit and exhibit too much impedance.

7.4 Internal error – continuous red LED

If the status LED is continuously red that means that the system has an internal error.

1. Wait for 5 minutes to see if the red LED remains. The system will try to recover automatically from internal errors.

2. Restart the system by a soft-reset by short-pressing the reset button (labelled number 11 in Figure 1).

3. Login to the Control Unit’s web interface and check for any error messages on the Network page.

7.5 SCG Control Unit Connector program shows the Control Unit, but it won’t open in the browser

The SCG Control Unit Connector program successfully finds the Control Unit. But when clicking “Open Selected Control Units” the web browser fails to open the CU’s configuration interface. This can happen when CU and laptop have IP-addresses in different ranges. This can be solved by the following these steps:

1. Make sure that the laptop is directly connected to the CU via a network cable. Both CU and laptop must not be connected to any other network.

2. Disable the Wi-Fi connection on the laptop

3. Restart the CU

4. Restart the laptop

5. Open the SCG Control Unit Connector program and click “Find Control Units”.

6. Select the Control Unit in the list and click “Open Selected Control Units”.

APPENDIX A: PRODUCT SPECIFICATIONS

The product specification of the Control Unit and the Sensor Unit can be downloaded here: https://www.dnv.com/scg2downloads/.

APPENDIX B: OVERVIEW OF STANDARDS

Standard	Test description	Test level
AC power		
IEC 61850-3 (subclause 3.54)	Rated voltage (IEC 60255-27, subclause 3.54]	120/230Vac nominal, 96Vac (80%) to 253Vac (110%)
Environmental		
IEC61850-3 (Table 18)	Dry heat operating (IEC 60069-2-2)	Test Bd 4h power-up, 16h steady-state, temp. +55˚C
IEC 61850-3 (Table 19)	Cold operating (IEC 60068-2-1)	Test Ad 4h power-up, 16h steady-state, temp. -10˚C
IEC 61850-3 (Table 20)	Dry heat storage (IEC 60068-2-2)	Test Bd duration 16h, temp. +70˚C
IEC 61850-3 (Table 21)	Cold storage (IEC 60068-2-1)	Test Ab duration 16h, temp. -25˚C
IEC 61850-3 (Table 22)	Temperature Cyclic (IEC 60068-2-14)	Test Nb -10˚C to 55˚C, 1˚C/min., 3h dwell time, 5 temp. cycles
IEC 61850-3 (Table 23)	Damp heat steady state (IEC 60068-2-78)	Test Cab Duration 10days, relative humidity 95%, 40˚C
IEC 61850-3 (Table 24)	Damp heat Cyclic (IEC 60068-2-30)	Test Db 25˚C to 55˚C, rel. humidity 95%, 24h per cycle, 6 cycles
IEC 61850-3 (Table 1) Clause 6.10.1	Vibration response (IEC 60255-21-1)	Normal environnement conditions, Class 1 10-59Hz, 0.035mm displacement amplitude 59-150Hz, 0.5g_n, 1 sweep per axis, 1 sweep = 8 min.
IEC 61850-3 (Table 1) Clause 6.10.1	Vibration endurance (IEC 60255-21-1)	Normal environment conditions, Class 1 10-150Hz, 1.0g_n, 20 sweep per axis, 160 min per axis
IEC 61850-3 (Table 1) Clause 6.10.2	Shock response (IEC 60255-21-2)	Normal environment conditions, Class 1 5g_n, duration 11 ms, 3 shocks in each direction
IEC 61850-3 (Table 1) Clause 6.10.2	Shock endurance (IEC 60255-21-2)	Normal environment conditions, Class 1 15g_n, duration 11 ms, 3 shocks in each direction
IEC 61850-3 (Table 1) Clause 6.10.2	Bump test (IEC 60255-21-2)	Normal environment conditions, Class 1 10g_n, duration 16 ms, 1000 pulses in each direction
IEC 61850-3 (Table 1) Clause 6.10.3	Seismic (IEC 60255-21-3)	Normal environment conditions, Class 1 1-8/9Hz, peak displacement=3.5mm, y=1.5mm 8/9Hz to 35Hz, peak acceleration x=1gn, y=0.5gn 1 sweep per axis
	Drop and topple test (IEC 60068-2-31)	Dropping onto a face Dropping onto an edge or a corner Toppling (pushover)
	IP31 (IEC 60529)	The CU shall comply with ingress protection level 31: Solid particle protection level 3 Liquid ingress protection level 1
	IP40 (IEC 60529)	The SU shall comply with ingress protection level 40: Solid particle protection level 4 Liquid ingress protection level 0
EMC		
IEC 61850-3 (Table 16)	Radiated Emission (CISPR 22 / IEC 55022)	Class A, Enclosure port @ 10m 30-230MHz, quasi-peak 40dB(µV) 230-1000MHz, quasi-peak 47dB(µV)
IEC 61850-3 (Table 17)	Radiated Emission (CISPR 22 / IEC 55022)	Class A, Enclosure port @ 3m 1-3GHz, average 56 dB(µV), peak 76dB(µV)

		3-5GHz, average 60 dB(µV), peak 80dB(µV)
IEC 61850-3 (Table 14)	Conducted Emission (CISPR 22 / IEC 55022)	Level A, Aux power supply test 0.15-0.5MHz quasi-peak 79dB(µV), average 66dB(µV) 0.5-30MHz quasi-peak 73dB(uV), average 60dB(µV)
IEC 61850-3 (Table 15)	Conducted Emission (CISPR 22 / IEC 55022)	Level A, Telecommunication ports 0.15-0.5MHz quasi-peak 84-74dB(µV), average 74-64dB(µV), quasi-peak 40-30dB(µA), average 30-20 dB(µA) 0.5-30MHz quasi-peak 7dB(µV), average 64dB(µV), quasi-peak 30dB(µA), average 20 dB(µA)
IEC 61850-3 (Table 9, Location H)	Electrostatic Discharge (IEC 61000-4-2)	Level 3 6kV contact, 8kV air
IEC 61850-3 (Table 9, Location H)	Electromagnetic fields (IEC 61000-4-3)	Level 3 80MHz - 3000MHz 10V/m
IEC 61850-3 (Table 10, Location H)	Fast transient/burst (IEC 61000-4-4)	Immunity, signal ports (LAN port) Level x 4.0 kV CM L/E & N/E
IEC 61850-3 (Table 11, Location H)	Fast transient/burst (IEC 61000-4-4)	Immunity, AC input Level 4 4.0 kV CM L/E & N/E
IEC 61850-3 (Table 13, Location H)	Fast transient/burst (IEC 61000-4-4)	Immunity, Functional earth >3m Level 4 4.0 kV CM L/E & N/E
IEC 61850-3 (Table 10, Location H)	Damped Oscillatory wave (IEC 61000-4-18)	Level 3, Signal ports (LAN port) Common mode = 2.5kV Differential mode = 1.0kV
IEC 61850-3 (Table 11, Location H)	Damped Oscillatory wave (IEC 61000-4-18)	Level 3, AC input Common mode = 2.5kV Differential mode = 1.0kV
IEC 61850-3 (Table 10, Location H)	Surge 1.2/50us (IEC 61000-4-5)	Level 4, Signal ports (LAN port) 4.0kV LE, 2.0 kV LL
IEC 61850-3 (Table 11, Location H)	Surge 1.2/50us (IEC 61000-4-5)	Level 4, AC input 4.0kV LE, 2.0 kV LL
IEC 61850-3 (Table 10, Location H)	Conducted disturbances (IEC 61000-4-6)	Level 3, Signal ports (LAN port) 10V, 150kHz 80MHz AM 80% 1kHz
IEC 61850-3 (Table 11, Location H)	Conducted disturbances (IEC 61000-4-6)	Level 3, AC input 10V, 150kHz 80MHz AM 80% 1kHz
IEC 61850-3 (Table 13, Location H)	Conducted disturbances (IEC 61000-4-6)	Level 3, Functional earth 10V, 150kHz 80MHz AM 80% 1kHz
IEC 61850-3 (Table 9, Location H)	Power Frequency magnetic field (IEC 61000-4-8)	Level 5, Immunity - Enclosure ports 50Hz 100A/m continuous
IEC 61850-3 (Table 9, Location H)	Power Frequency magnetic field (IEC 61000-4-8)	Level 5, Immunity - Enclosure ports 50Hz 1000A/m for 1sec
IEC 61850-3 (Table 11, Location H)	Voltage Dips (IEC 61000-4-11)	Immunity, AC input ΔU 60% for 50 periods

IEC 61850-3 (Table 11, Location H)	Voltage Interruptions (IEC 61000-4-11)	Immunity, AC input ΔU 100% for 50 periods
Safety		
IEC 61850-3 (subclause 6.6.3)	Impulse voltage withstands (IEC 60255-27 subclause 10.6.4)	AC input 1.2/50 µs; 5 kV
IEC 61850-3 (subclause 6.6.3)	Impulse voltage withstands (IEC 60255-27 subclause 10.6.4)	Communication port 1.2/50 µs; 1 kV
IEC 61850-3 (subclause 6.6.4)	Power frequency dielectric withstand voltage (IEC 60255-27 subclause 10.6.4)	AC input 2kVac; 50Hz; 1 minute
IEC 61850-3 (subclause 6.6.4)	Power frequency dielectric withstand voltage (IEC 60255-27 subclause 10.6.4)	Communication port 0.5kVac; 50Hz ; 1 minute
IEC 61850-3 (subclause 6.9.2.2)	Insulation resistance (IEC 60255-27 subclause 10.6.4)	AC input >100 MΩ at 500Vdc before damp heat test >10 MΩ at 500Vdc after damp heat test
IEC 61850-3 (subclause 6.6.1)	Creepage & clearance (IEC 60255-27 subclause 10.6.3)	Pollution degree 2 & Overvoltage Category 3
IEC 61850-3 (subclause 6.6.5)	Protective bonding (IEC 60255-27 subclause 10.6.4.5)	<0.1Ω
IEC 61850-3 (subclause 6.6.6)	Flammability (IEC 60255-27 subclause 10.6.5.2)	No risk of fire
IEC 61850-3 (subclause 6.6.7)	Single fault (IEC 60255-27 subclause 10.6.5.5)	No risk of electrical shock or fire

APPENDIX C: NETWORKING BETWEEN LAPTOP AND CONTROL UNIT

When a laptop is directly connected to the Control Unit there is no DHCP server that will hand out IP-addresses. The Control Unit will automatically assign itself a random address from the link-local range (169.254.0.0/16) (https://en.wikipedia.org/wiki/Link-local_address). The laptop must also pick an address from this range. This is the standard configuration for most operating systems. In Windows make sure that the Internet protocol TCP/IP of the used network adapter has the following options selected: "Obtain an IP address automatically" and "Automatic private IP address". These are the Windows default options.

When both the Control Unit and laptop have an address from the same range, the laptop must determine the IP address of the Control Unit. The Control Unit will respond to Multicast DNS (mDNS) (https://en.wikipedia.org/wiki/Multicast_DNS) requests. The SCG Connector app (https://www.dnv.com/scgsupport/) program will perform these requests. For this, the firewall on the laptop must allow the following connection:

1. Outbound request from laptop to Control Unit:
    (a) Protocol: UDP
    (b) Source IP: 169.254.0.0/16 (laptop's own IP address)
    (c) Source port: any
    (d) Destination IP: 224.0.0.251
    (e) Destination port: 5353

A stateful firewall, such as the standard Windows firewall, will automatically allow the reply from the Control Unit to the laptop. If the firewall does not automatically allow the response, then the following rule must be added.

2. Inbound answer from Control Unit to laptop:
    (a) Protocol: UDP
    (b) Source IP: 169.254.0.0/16 (any address in 169.254.*.* range)
    (c) Source port: 5353
    (d) Destination IP: 224.0.0.251
    (e) Destination port: 5353.

About DNV

DNV is the independent expert in risk management and assurance, operating in more than 100 countries. Through its broad experience and deep expertise DNV advances safety and sustainable performance, sets industry benchmarks, and inspires and invents solutions.

Whether assessing a new ship design, optimizing the performance of a wind farm, analyzing sensor data from a gas pipeline or certifying a food company's supply chain, DNV enables its customers and their stakeholders to make critical decisions with confidence.

Driven by its purpose, to safeguard life, property, and the environment, DNV helps tackle the challenges and global transformations facing its customers and the world today and is a trusted voice for many of the world's most successful and forward-thinking companies.