@ccess the Ethernet

USER GUIDE

SCX2e

GS2

arcutronix GmbH
Deutschland

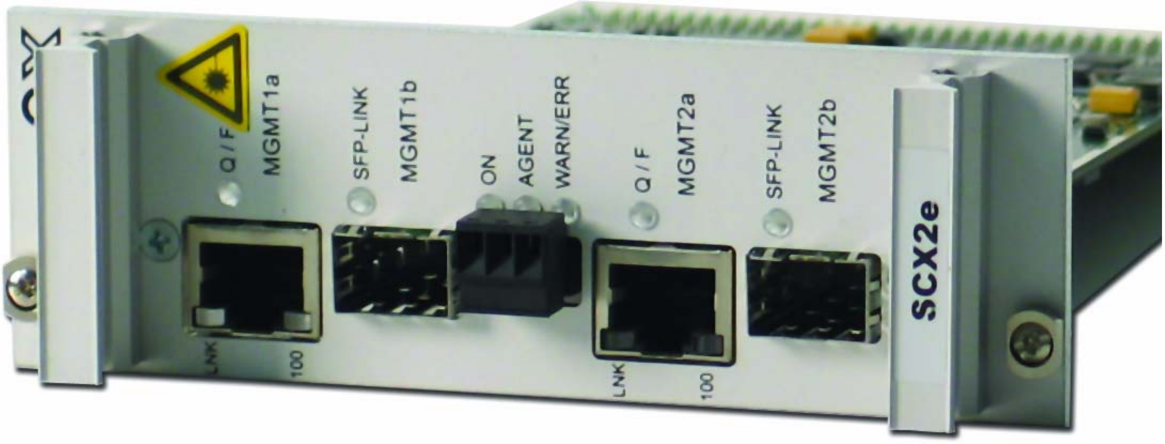
Installation and Operation Manual

Version 2.1

arcutronix

SCX2e - System Controller

USER GUIDE



Covered Variants of SCX2e by this User Guide:

SCX2e	0903 - 3000 / GS2
SCX2e-WDM	0903 - 3010 / GS2

Covered Software Versions of SCX2e by this User Guide:

SW-Version (≥):	V 2_0_01
Boot-Loader (≥):	V 1_2

Part-Number (User-Guide):	0903 30 65.man
Version:	V 2.1
Date of Issue:	2014-08-07

Contacts

arcutronix GmbH
Garbsener Landstraße 10
D-30419 Hannover, Germany
Tel.: +49 (0)511 277- 2700
Fax: +49 (0)511 277- 2709
E-Mail: info@arcutronix.com
http://www.arcutronix.com

Copyright Note

Document Contents

This document contains the latest information available at the time of publication. The content of this document is subject to change without prior notice. arcutronix reserves the right to modify the content at any time. arcutronix shall not be liable for errors contained herein or for incidental or consequential damages in connection with the furnishing, performance, or use of this material. To request arcutronix publications or comment on this publication, contact a arcutronix representative or the arcutronix corporate headquarters. arcutronix may, without obligation, use or distribute information contained in comments it receives. Address correspondence to the attention of Manager, Technical Publications.

Trademarks

About this Book

Document Organization

This guide describes the hardware and software components of the SCX2e - System Controller. It provides information on configuration, system installation and technical data.

The intended audience of this document is anyone who is responsible for installing, maintaining or operating the SCX2e - System Controller. This person must be aware of the risks, affected with these actions and must be qualified and trained. **Observe the safety precautions in chapter "Safety, Instructions, Statements".**

The manual is designed as printable book, therefore chapters start at an odd page (the last even page of the chapter before may be empty). The headlines of the pages contain chapter name, chapter count, and chapter headline. The foot lines of the pages contain chapter page count, the revision date and the document title.

Chapters

Chapter 0**, Safety, Instructions, Statements:** Handling, precautions, warnings.

Chapter 1**, Abstract:** General description of the SCX2e devices and applications for use.

Chapter 2**, Getting Started:** Short form about installation, mounting and configuration of SCX2e-family.

Chapter 3**, Hardware & Interfaces:** Description of hardware and front panel elements.

Chapter 4**, Functionality:** Switching, routing, agent.

Chapter 5**, SCX2e Web-GUI:** Control and configuration of the SCX2e.

Chapter 6**, SNMP and MIBs:** Remote monitoring of the SCX2e.

Chapter 7**, SSH and CLI:** Explains the SSH access to the SCX2e and the usage of the Command Line Interface (CLI).

Appendix A**, Technical Specifications:** Technical data of the SCX2e.

Appendix EC**, EC Declaration of Conformity:** Valid for the SCX2e product family.

Conventions

This manual uses the following text conventions to convey instructions and information:

Normal text is written in Albany font.

Commands and Arguments are done in `Courier New`.

Notes, cautions, and tips use these conventions and symbols:

NOTE: Means reader take note. Notes contain helpful suggestions or references to materials not contained in this manual.

WARNING:

⚠ DANGER

Means reader be careful. In this situation, you might do something that could result in equipment damage or loss of data.

Release History

2014-08-07	Version 2.1	Editor: mjz

Added and changed the following topics:

- WebGUI-RefGuide and CLI-RefGuide are now extra documents to reduce size of this manual.

2012-07-01	Version 2.0	Editor: mjz

Added and changed the following topics:

- New HW version “GS2” available for SCX2e - System Controller. This new HW supports more flexibility in Ethernet interfaces and fits better for SCX2e-WDM.

Referenced and Related Documents

[axRefGuideWebGUI_SCX2e] arcutronix GmbH (2014): SCX2e Web-GUI, Reference Guide.

[axRefGuideCLI_SCX2e] arcutronix GmbH (2014): SCX2e Command Line Interface, Reference Guide.

[IEC 60825-1] IEC 60825-1 - 2007: Safety of laser products - Part 1: Equipment classification and requirements

[IEEE 802.1AS] IEEE Std 802.1AS™-2011: Timing and Synchronization for Time-Sensitive Applications in Bridged Local Area Networks.

[IEEE 802.1AX] IEEE Std 802.1AX™-2008: Link Aggregation.

[IEEE 802.1D] IEEE Std 802.1D™-2004: Media Access Control (MAC) Bridges.

[IEEE 802.1Q] IEEE Std 802.1Q™-2011: Media Access Control (MAC) Bridges and Virtual Bridge Local Area Networks.

[IEEE 802.3] IEEE Std 802.3™-2008: Part3: Carrier sense multiple access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications.

[IETF RFC 791] IETF RFC 791 (1981), Internet Protocol (IP).

[IETF RFC 1305] IETF RFC 1305 (1992), Network Time Protocol (Version 3) Specification, Implementation and Analysis.

[IETF RFC 1350] IETF RFC 1350 (1992), The TFTP Protocol (Revision 2).

[IETF RFC 1901] IETF RFC 1901 (1996), Introduction to Community-based SNMPv2.

[IETF RFC 3410] IETF RFC 3410 (2002), Introduction and Applicability Statements for Internet Standard Management Framework.

[IETF RFC 3414] IETF RFC 3414 (2002), User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3).

[IETF RFC 4251] IETF RFC 4251 (2006), The Secure Shell (SSH) Protocol Architecture.

[IETF SFTP] IETF draft-ietf-secsh-filexfer-13 (2006), SSH File Transfer Protocol.

[INF-8074i] SFF Commitee, INF-8074i Specification for SFP (Small Formfactor Pluggable) Transceiver, Rev 1.0, May 12, 2001

[INF-8077i] SFF Committee, INF-8077i 10 Gigabit Small Form Factor Pluggable Module, Revision 4.5, August 31, 2005

[ITU-T Y.1731] Recommendation ITU-T Y.1731 (2006), OAM functions and mechanisms for Ethernet based networks.

[SFP MSA] Small Form-factor Pluggable (SFP) Transceiver Multi Source Agreement (MSA) (2000)

List of Contents

Chapter 2 Getting Started

Chapter 3 Hardware & Interfaces

Chapter 4 Functionality

Chapter 5 SCX2e Web-GUI

Chapter 6 SNMP and MIBs

Chapter 7 SSH and CLI

Appendix A Technical Specifications

Appendix EC EC Declaration of Conformity

List of Figures

List of Tables

Chapter 0
Safety, Instructions, Statements

Safety Precautions

The following sections provide the safety precautions for the supplied device. You must always observe the power precautions for the device. You must follow all warning notes to ensure that the procedures are performed safely. You must follow all caution notes to ensure that the device is operated correctly.

WARNING: Serious injury or loss of life is possible, if instructions are not carried out.

CAUTION: Serious damage or destruction is possible, if instructions are not followed.

NOTE: Before installing the device find out if any local technical rules must be observed. These may be defined by ANSI, ITU, IEC, your PTT, or other similar organizations.

Power Precautions

WARNING:

DANGER

- Disconnect the power cord before opening the device.
- Always plug the power cords into properly grounded receptacles. An improperly wired receptacle could place hazardous voltage on the accessible metal parts of the device.
- Use only approved power cords.
- Use only manufacturer supplied power supplies.
- The power supply must match the power specifications for the device.
- Do not work on the equipment during periods of lightning activity.

Handling Precautions

Note: Precautions for transporting, installing, and operating the device:

- Avoid excessive shocks and vibrations. Install shock absorbers, if you need to use the device for mobile applications.
- Avoid contact with any liquid (e.g. water) or dust or dirt.
- Avoid exposing the device to excessive direct sunlight.

- Ensure sufficient cooling of the device.
- Prevent loose items from falling into the device.
- Avoid damage to components when installing or setting switches or jumpers of the device.
- Always place protective covers on all fibre optic cables and connectors that are not in use to prevent breakage and contamination.
- Inspect all fibre optic connections and clean contaminated surfaces before use.
- Attach a wrist strap and follow ESD procedures, see next paragraph.

Preventing Damage From Electrostatic Discharge

CAUTION: Discharge of static electricity (ESD) can damage or degrade electronic components. The electrostatic potential of a person can be several thousand Volt and a discharge to semiconductor components may have severe consequences. Observe the precautions below when you are handling any hardware with electronic components.

Card Protection

Each card is shipped in a separate, reusable, and anti-static shielding bag. Leave each card in its bag until you are ready to install it into the system. Do not remove the card from its bag unless you are grounded. Do not place a bag on exposed contacts where it can cause short circuits.

Grounding Procedure

Before attempting to install or remove any part of the chassis, ensure that you, the equipment chassis, and the rack mount cards are at ground potential to prevent electrostatic discharge (ESD). Electrostatic discharges can damage the components of the system. To place yourself at ground potential, connect the chassis with a ground wire or via the power cord with a grounded mains socket and clip your wrist strap to the chassis.

The following advice will help you to prevent ESD damage to electrical components:

- Always use an ESD wrist strap with a metal clip for grounding.
- Limit your movement as much as possible. Movement can cause a build-up of static electricity.
- Handle the system and its components carefully. Never touch the circuitry. Place your hands only on the edges, rails, or frame of the unit.
- Touch a spare component - while it is still in the anti-static wrapping - to an unpainted metal portion of the chassis for at least two seconds. This allows the static electricity to discharge harmlessly from your body and the spare.
- Install the spare directly into the chassis after removing it from the anti-static wrapping. Do not remove the anti-static wrapping until you are ready to do the install. If you must set down an unwrapped spare, set it down on an anti-static mat or on its anti-static wrapping.

Caution: Do not place the spare component on the top of the chassis (rack) or on a metal table. Either action could cause severe damage to the spare.

- Set down cards with their component sides face up.
- Be aware of weather conditions. Cold weather increases the likelihood of static electricity build-up.
- Be aware of your own conductivity level. Wear ESD shoes to diminish personal static electricity build-up. Wear e.g. an electrostatic dissipative lab coat.

Fibre Optic Precautions

Caution: An optical fibre may carry (invisible) light from the remote system.

This device may contain Laser Class 1 components, like laser transmitters or light emitting diodes LED (refer to technical data). Operating components emits (invisible) laser radiation. Be careful when you are working with these components. The following safety precautions must be followed when working with fibre optics and Laser Class 1 components:

WARNING: Do not look into the fibre optic output. Looking into the fibre optic output can cause injury to the eye. When observation is necessary eye protection must be worn and precautions must be taken to avoid exceeding the limits recommended in ANSI Z136.1-1981.

WARNING: Use caution when working with the laser components of the device. The device is designed to protect the user against optical powers beyond laser class 1.

WARNING: Ensure that the incoming signal from the remote device does not exceed the power defined for laser class 1 when the cabling is disconnected. The device will also become unsafe, if any unsafe equipment is connected to the system.

WARNING: Do not disconnect the fibre optic cables while power is applied. Disconnecting the fibre optic cables could expose the user to optical powers beyond laser class 1.

Caution: Use Of Controls Or Adjustments Or Performance Of Procedures Other Than Those Specified Herein May Result In Hazardous Laser Light Exposure.

CAUTION Laser Class 1. Complies with FDA radiation standards, 21CFR subcategory J. DANGER (Invisible) laser radiation when open and / or interlock defeated. Avoid direct exposure to beam!

Technical Instructions to User

Do not use this product for other applications than suggested in this manual!

The international standards and the technical rules of your local PTT company must be observed.

All interface cables to this equipment must be shielded and designed in accordance with proper EMI techniques to ensure compliance with EMC requirements. arcutronix will provide cable shielding specifications on request.

Inspection

Before commissioning, check the content of the consignment for completeness and note whether any damage has occurred during transport. If so, do not use the parts and contact your arcutronix representative.

Commissioning

Work may be carried out only by qualified personnel. The relevant precautions must be taken.

Cleaning

To clean the outer surfaces, use a soft damp (not wet) cloth. Do not let moisture go inside. Please consider the properties of the housing and other material used!

Table 0-1 *Effects of Cleaning Liquids*

Valuation	ABS/ABS+PC/PC/PPE+PS
well resistant	water, aqueous saline solutions, sud, diluted acid and alkali
conditionally resistant	alcohol, aliphatics, oil and fat
not resistant	concentrated mineral acid, aromatic and halogenated hydrocarbon, ester, ether, ketone

Quality

The quality management of arcutronix GmbH is certified to DIN ISO 9001:2000.

This product is manufactured to the arcutronix GmbH quality standards.

Repair

There are no repairable parts in the device. Defective parts must be sent to arcutronix GmbH for repair. The power supplies of a device may contain fuses. Blown-up mains fuses must be replaced by fuses of the same type and the same ratings. Using repaired fuses or short-circuit the fuse holder are not permitted.

Disposal and Recycling

This symbol on the product or on the packaging indicates that it is can be recycled. To save our environment please hand it over to your next recycling point.

This symbol on the product or on its packaging indicates that it shall not be treated as household waste. Instead it shall be handled over to the applicable collection point for the recycling of electronic equipment.

For more detailed information about recycling contact your local city office, your waste disposal service or where you purchased the product.

CE Conformity

arcutronix products complies with the European standard regulation. They are tested to the Council guideline for harmonizing the legal regulations of the member states on electromagnetic compatibility.

Electromagnetic Immunity Statement

This equipment has been tested and found to comply with the limits of EN 50082-2 (Electromagnetic Immunity for heavy industry).

Instructions to User

All interface cables to this equipment must be shielded and designed in accordance with proper EMI techniques to ensure compliance with EMC requirements. arcutronix will provide cable shielding specifications on request.

Electromagnetic Emissions Statements

To achieve satisfactory EMC performance, all interface cables to this equipment must be shielded and designed in accordance with proper EMI techniques. Rack mount cards has to be inserted into the designated chassis. Chassis slots that are not used have to be covered with a blanking plate. The chassis must be bonded to earth. This is usually achieved by installing the power cord to the chassis. An extra earth terminal may be provided. If this device is used in a residential setting, resulting interference must be corrected by the user. Any user modification made to the unit voids the user's authority to operate the unit under the FCC rules.

WARNING: This is a Class A product. In a domestic environment, this product may cause interference in which case the user may be required to take adequate measure. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

United States Federal Communications Commission (FCC) Electromagnetic Emissions Statement

WARNING: This equipment generates, uses, and can radiate radio frequency energy and if not installed and used in accordance with the instructions in this manual, may cause interference to radio communications. It has been tested and found to comply with the limits for a Class A computing device pursuant to Subpart J of Part 15 of the FCC Rules, which are designed to provide reasonable protection against such interference in which case the user at his own expense will be required to take whatever measures may be required to correct interference.

Canadian Department of Communications (DOC) Statement

WARNING: This equipment generates, uses, and can radiate radio frequency energy and if not installed and used in accordance with the instructions in this manual, may cause interference to radio communications. This digital apparatus has been tested and does not exceed the Class A limits for radio noise for digital apparatus set out in the DOC Radio Interference Regulations. The regulations are designed to provide reasonable protection against radio noise interference in which case the user at his own expense will be required to take whatever measures may be required to correct interference.

European Communities

WARNING: This equipment has been tested and found to comply with the limits of CISPR 22 and EN 55022 Class A for information technology equipment. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications.

Chapter 1
Abstract

SCX2e Description

General

The System Controller SCX2e is used to control and configure all types of managed arcutronix line-cards: Connectivity, Transport and Ethernet service types. The SCX2e allows the administrator and operator to configure and monitor local as well as remote devices via one single access point.

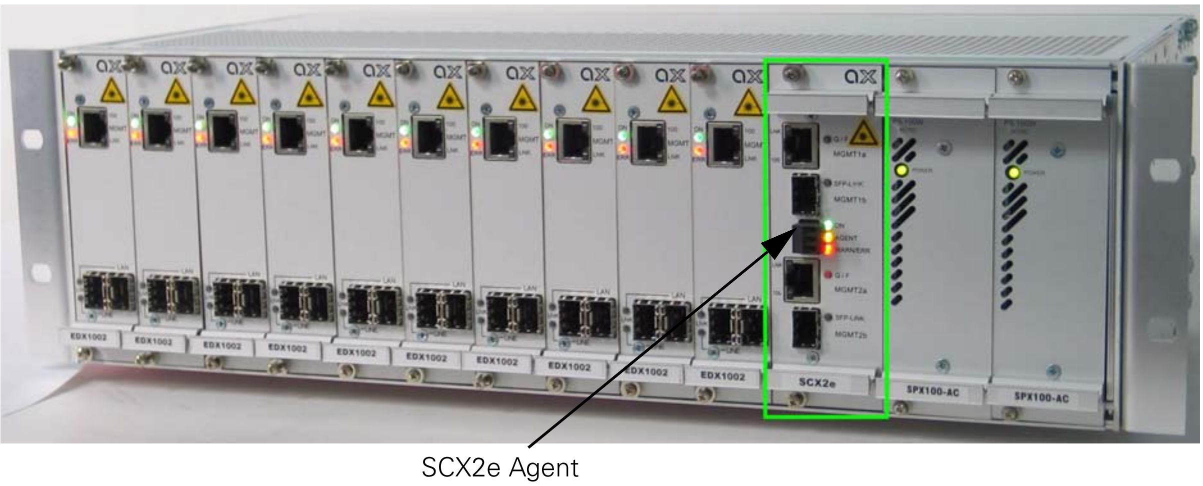


Figure 1-1 *SCX2e in ax 10-slot Chassis SRX10*

The SCX2e is used in multi-slot as well as is in single-slot chassis. A multi-slot chassis offers the capacity of 3, 10 or 24 line-cards. The SCX2e communicates with the plugged line-cards across the back-plane and can set and read the management attributes of the cards. The agent itself has some global measurement units on-board to check the system-power, the temperature and optional fans. This makes it a powerful device, not only the manage the line-cards, but the whole chassis and the incorporated units. A single-slot chassis in this context is a housing offering one (single) slot for a line-card plus one (single) slot for the agent-card. So in fact, there are two slots, only one of both can be used for line-card. The second slot is dedicated for the agent, only. One example for a single-slot chassis in this context is the SHX3-SC.

The System Controller SCX2e provides access by very different methods to fit into a wide bunch of applications and management scenarios. Some of these are

- Four Ethernet ports to have 2x copper and 2x fibre access options,
- Web-GUI for an intuitive and user-friendly way,
- Command Line Interface for scripting and automation,
- SNMP-agent for alarm-push and integration in umbrella management systems, and
- SSH-2 for high security.

Web-GUI and local management assist a user friendly field installation and configuration. For SNMP management, several standard and product specific MIB files (Management Information Base) are provided.

SNMP management can be interconnected to any SNMP-compatible management software such as HP Open View and SNMPc (Castle Rock).

Remote SW-upload for SCX2e and each other component in the system rack is realized via HTTP or FTP [1]. After copying SW updates to SCX2e Flash File System, updated files are loaded into agent and plugged modules on administrator request.

The given management capabilities allow Carriers and ISPs to maintain and supervise all devices inside management system via single NMS access point. Trap signalling helps to detect errors in case of any failure or status change at the local and remote site.

Application areas for SCX2e

The SCX2e is a (pluggable) agent card, which offers centralized management access for different arcutronix access- and metro-systems. An arcutronix system is always a bundle of line-cards, which offer very different types of services, plus the incorporating housing, power supply etc. In some systems, the SCX2e is fixed mounted, while in others it is pluggable. The number of interfaces for management access may vary in the different applications, but the provided feature set, with respect to the agent's main tasks, are always the same.

The SCX2e has some pre-defined configurations, which can be easily loaded. These configurations are intended to fit the SCX2e in special application-scenarios and each configuration assigns several settings in one step. This makes it easy to fit the device and reduces possible problems due to bad configurations.

Other applications can be configured manually, but care must be taken to setup the unit in the correct way and to avoid bad configurations. The device does check as much as possible before it accepts new settings, but not all can be proved. Some configurations might be allowed, but not meaningful in the given context. Loss of communication with the device might be a result.

In the following the pre-defined setups will be presented and roughly depicted.

[1] TFTP and SFTP are supported.

“Daisy Chain”

This setup is intended to be used in locations, were several multi-slot chassis are installed. The remote management access to this location must only be done once and the different agents are then cascaded in a daisy chain. In total there are 3 logical interfaces:

- 1x Combo-port (= 1x Copper Ethernet plus 1x SFP port),
- 1x pure copper Ethernet interface and
- 1x pure SFP interface.

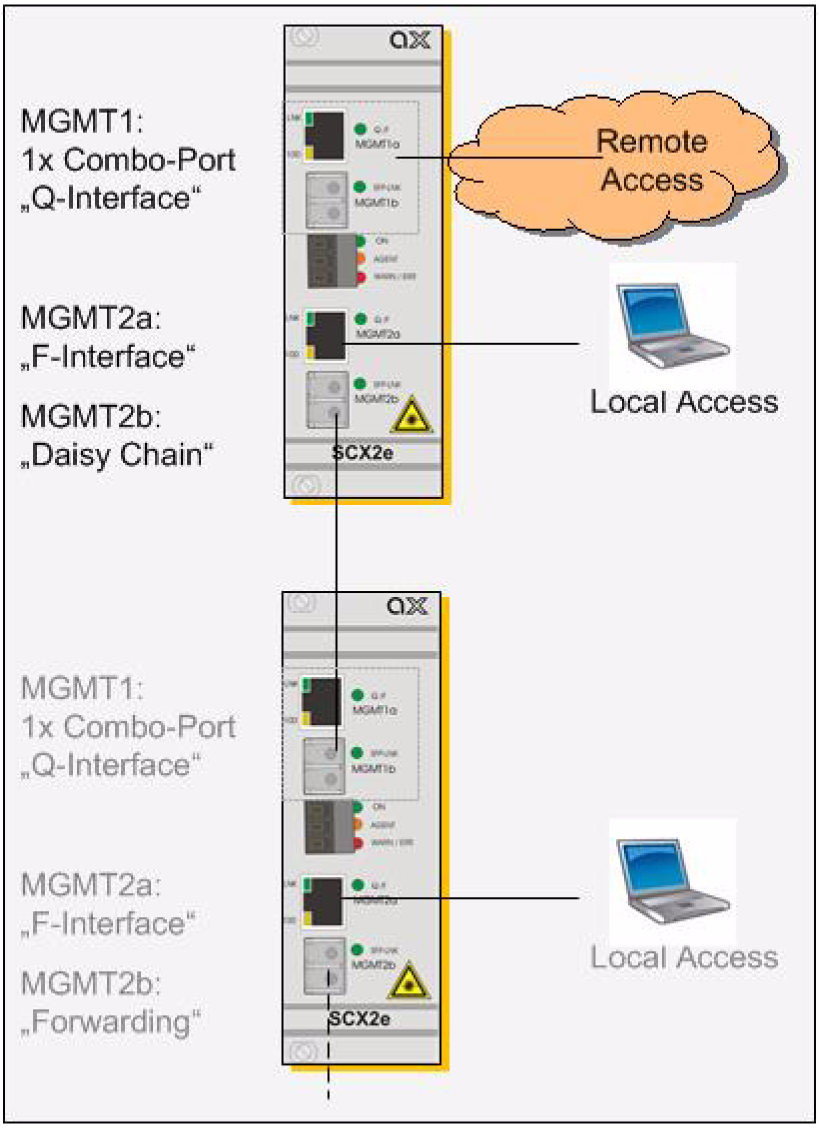
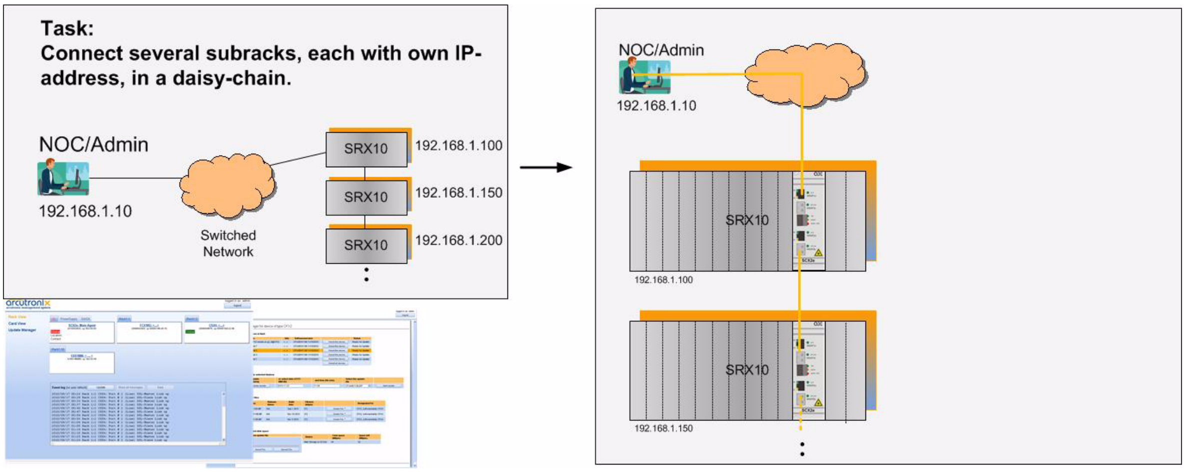


Figure 1-2 *Daisy Chain*

The two ports MGMT1a and MGMT1b are grouped together to one logical interface, a so-called Combo-port. The combo-port is intended to be used for remote access, and is operated in the “Q-mode”. This means, the interface has an IP-address and is waiting to get this IP-address from the network’s DHCP-server.

The copper port (MGMT2a) is good for local management access, it has also an IP-address and can provide an IP-address to an attached laptop/PC via DHCP. This interface is acting in the “F-mode”.

The SFP port is pre-configured as a “Forwarding” port and can be used to attach the next agent in the chain. As all SFP ports do support as well fibre optic SFPs as well as copper SFPs, the daisy-chain can be short-haul (copper) or long-haul (fibre).



Task:
Connect several subracks, each with own IP-address, in a daisy-chain.

***Figure 1-3** SCX2e Management Application “Daisy Chain”*

The setup “Daisy Chain” may be mixed up with different settings on other agents. There is no need to have all agents of the same configuration within one network.

“Remote Management”

The setup “Remote Management” is only available on the SCX2e-WDM agent. It is intended to offer remote management via a small WDM-overlay network, build with the WDM-filter onboard this special HW-variant of the agent. A fibre based service, which needs remote management across the same fibre (as the service itself), can make use of the WDM capability. Service traffic and management traffic are multiplexed on the same line without any interference or decrease of bandwidth.

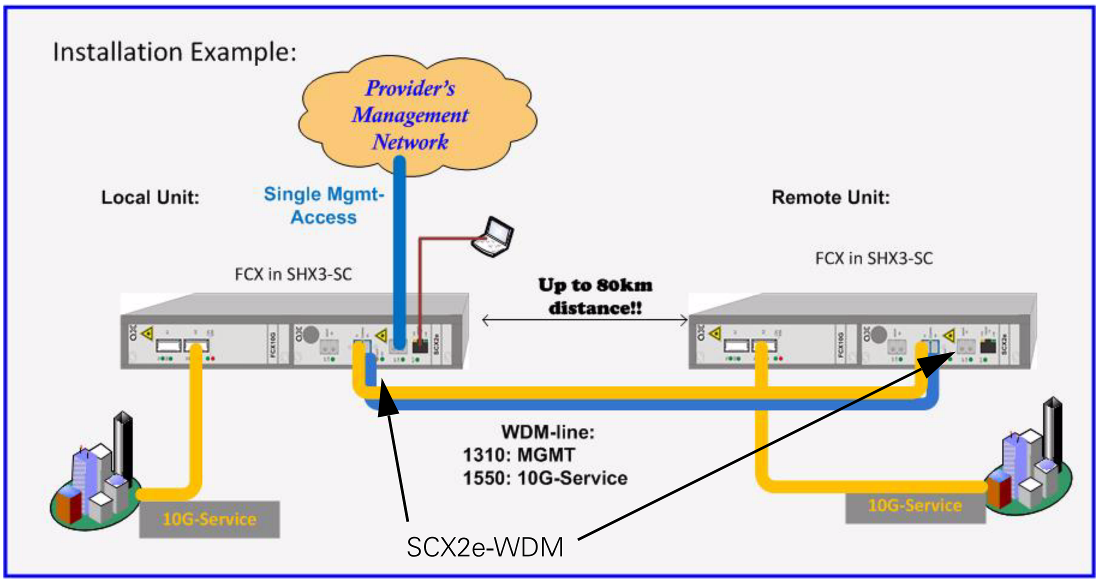


Figure 1-4 *SCX2e-WDM Remote Management Application*

The SCX2e-WDM is intended to be only used in the double-slot housing SHX3-SC, which is shown in the figure above, too.

The WDM filter is a pure passive component, which is mounted on the PCBA of SCX2e-WDM.

The SCX2e-WDM does have 3 Ethernet ports:

- One copper port for local management, only.
- One fibre-optic port to provider's management network (to NOC).
- One fibre port for WDM-overlay to peer.

SCX2e Functions at a Glance

The SCX2e rack agent allows the management of ax-chassis and expansion chassis equipped with rack mounted line-cards (LCs). It provides access by standard TCP/IP stack and any kind of management platform using SNMP, SSH or a web-browser. The chassis and the installed rack mount cards can be monitored and configured locally and remotely.

The SCX2e communicates with the arcutronix Multi Service System and installed rack mount cards and allows the following management features:

- Central management access device for system racks (SRX family)
- Up to 25 line-cards can be handled by one agent
- Auto-detection of equipped line-cards
- SW-upload for each component in a system rack via http or (T)FTP

- Flash File System, for saving new and old SW files of all plugged cards
- Various management access options: SNMP, Web-GUI, Telnet
- Power and Fan control functionality
- SNMP trap-signalling in case of local or remote status changes
- Discovery of system rack types
- Alarm relay - Enhanced alarm threshold selectable in addition to autonomous alarm function via alarm relay contacts on fan module
- Compact 3RU rack card
- Power supply via system racks (SRX) or Management-housing (SHX-SC)
- Temperature and power-supply supervision
- NTP support
- Time/date synchronisation of all line-cards within the chassis.

Alarming

Alarm conditions can be detected depending on the settings made in the control software. Each SCX2e card monitors all power supplies and rack mount cards of the chassis and the fan’s function. If there is a failure recognized by an SCX2e card, an alarm will be set by the agent.When alarm condition is reached, several action (can) take place:

- Red Alarm-LED is ON,
- Alarm-Relay is closed,
- SNMP-trap is sent out (trap receiver must be configured correctly!).

Order Information

NOTE: All order matrices will be regularly updated. Asked your arcutronix representative for the latest publications.

Table 1-1 *Order Matrix*

Art.- No.	Short Name	Description
0903-3000	SCX2e	System Controller for connectivity system devices: • SNMP, Web-GUI, SSH, • 4x GigE-Ports (2x RJ45: 10/100/1000BaseT; 2x SFP: 1000Base-X), • with alarm contact, • 3RU rack mount card.
0903-3010	SCX2e-WDM	System Controller for connectivity system devices: • SNMP, Web-GUI, SSH, • 1x GigE-Port (RJ45: 10/100/1000BaseT), • 1x GigE-Port (SFP: 1000Base-X), • Onboard passive WDM filter (1310/1550nm std SM), • 3RU rack mount card.

Accessories

Housings and Cables

The arcutronix' Multi Service Platform offers a range of accessories for an easy and space saving installation of your device into 19" cabinets or as desktop / wall-mount installation.

Table 1-2 *Accessories Housings & Cables*

Art.- No.	Short Name	Description
0805-9000	SRX10	Rack mount shelf: • 19" chassis • Height: 3RU • 10 slots for line-cards • 1 slot for management • 2 slots for modular AC (115/230V) and/or DC (-48V) power supplies.
0805-9500 (obsolete!)	SRX24	Rack mount shelf: • 19" high density chassis • Height: 6RU • 24 slots for line-cards • 1 slot for management • 2 slots for modular AC (115/230V) and/or DC (-48V) power supplies.

Table 1-2 Accessories Housings & Cables (continued)

Art.- No.	Short Name	Description
0717-9501	SHX3-SC	Stand-alone housing: • 1x slot for 3RU line-card, • 1x slot for SCX2e-WDM Management card only, • max. 15W total power consumption, • VT100 Management port (D-Sub) • with alarm contacts, grounding bolt, ventilation, • integrated wide range power supply, • mains supply: 48VDC…110/230VAC, • DC jack included.
0500-001	PC-E	Power cord, European plug.
0500-002	PC-B	Power cord, Great Britain plug.

NOTE: All order matrices will be regularly updated. Asked your arcutronix representative for the latest publications.

SFPs (Small Form-factor Pluggable)

The SCX2e-series offers a number of SFP-slots (Small Form-factor Pluggable) for usage of a wide range of different optical transceivers. The small form-factor pluggable (SFP) is a compact, “hot-pluggable” optical transceiver used in optical communications for both telecommunication and data communications applications. The SFP transceiver is specified by a multi-source agreement (MSA) between competing manufacturers.

Using the right SFP, the SCX2e can be used in different optical environments with different fibre-types (single-mode or multi-mode) and a wide range of distances.

All SFP ports are compliant with [INF-8074i] and must be connected to SFP modules that are class 1 lasers and are compliant with [IEC 60825-1].

Two speed-rates of SFP-based interfaces are available: 100MBit/s and 1000MBit/s. For both speed-rates, arcutronix offers a bunch of different SFPs.

SCX2e does support all optical modules, which are designed according the SFP MSA. For safe operation, arcutronix recommends the SFPs below. Please ask for special types, if required.

Table 1-3 *Accessories SFPs*

Short Name	Description
Optical Transceiver:	
100Base-FX:	
SFP-155-S13-10	Optical SFP Interface Module: 1310nm SM FO; Fast E, 155 Mbps transceiver; pluggable SFP footprint; LC connector; 10km.
SFP-155-S13-15	Optical SFP Interface Module: 1310nm SM FO; Fast E, 155 Mbps transceiver; pluggable SFP footprint; LC connector; 15km
SFP-155-S13-40	Optical SFP Interface Module: 1310nm SM FO; Fast E, 155 Mbps transceiver; pluggable SFP footprint; LC connector; 40km.
1000Base-SX/LX/LH/ZX	
SFP-1.25-S13-10	Optical SFP Interface Module: 1310nm SM FO; 1xFC, 1.25 Gbps transceiver; pluggable SFP footprint; LC connector; digital diagnostics; 10km.
Copper Transceiver (Triple-Speed SFP):	
SFP-1.25e	Electrical SFP Interface Module: Pluggable SFP module, for data rates of 1.25Gb/s bi-directional data links. - 1000BASE-T Copper port, RJ45 connector - compatible with the Gigabit Ethernet and 1000BASE-T standards as specified in IEEE 802.3 - digital diagnostic supported.

Chapter 2
Getting Started

For the start-up of the SCX2e please follow the directions in this chapter.
You must keep the operating conditions specified for the devices. In the following read about the start-up preparation, the start-up itself, and the possibility to automate the start-up.

WARNING: Read the safety notes at the beginning of this manual carefully before you start the device!

Delivered Parts

Please check if all the items listed below are included in your delivery.
Your delivery includes:

- SCX2e System Controller Card,
- Short User-Information

Preparing the Start-up

Before you switch on the device you need to check the operating conditions and install the SCX2e into the chassis or the desktop-housing.

Operating Conditions

Read the operating conditions specified in this section carefully to avoid damages to the device or connected systems.

Ambient Conditions

The ambient conditions, which must be maintained for the SCX2e, are shown in Table 2-1.

Table 2-1 *Ambient Conditions*

Operating Temperature	5+°C to +55°C
Max. Relative Humidity (non-condensing)	<100% (30°C)

Table 2-1 Ambient Conditions (continued)

Input Voltage	+5V DC
Power Consumption	< 7 VA [i]

[i] Depends on the given variant and used SFPs.

CAUTION: If operating limits are exceeded, malfunctions and permanent damage to the equipment may result.

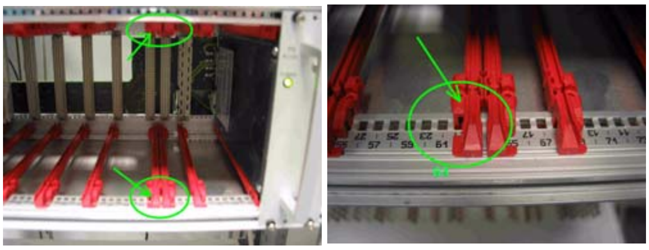
NOTE: In order to operate the various interfaces, please ensure that the plugs are firmly engaged in the sockets.

SCX2e Mounting

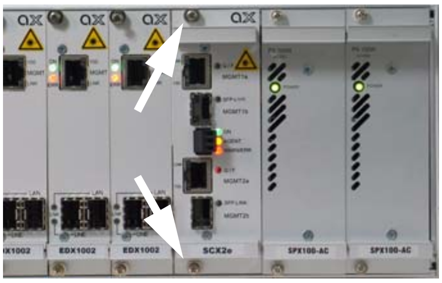
In SRX10

To mount the SCX2e into the ax-chassis SRX10 please follow the subsequent step-by-step instructions.

1. Disconnect all cables from the SCX2e before mounting the device.
2. Place the SCX2e right way up on a table with the front panel looking in your direction.
3. Insert the SCX2e that way into the chassis as shown below. Use slot with the rail number 63!



4. Fix the SCX2e to the housing using the provided screws.



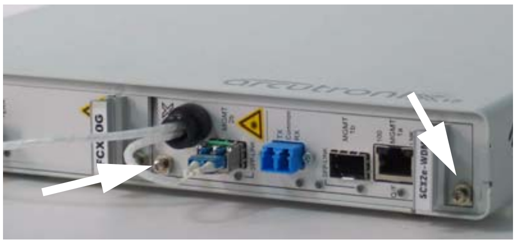
5. Connect the interface cables to the SCX2e.

In SHX3-SC

To mount the SCX2e or SCX2e-WDM into the ax-chassis SHX3-SC please follow the subsequent step-by-step instructions.

1. Disconnect all cables from the SCX2e before mounting the device.
2. The SCX2e is mounted in horizontal way, the handle must be on the right side.
3. Insert the SCX2e into the right slot of the SHX3-SC, only.

4. Fix the SCX2e to the housing using the provided screws.



5. Connect the interface cables to the SCX2e.

In SRX3plus

In the SRX3plus, the agent-card is mounted internally and one can neither remove nor install the agent. A replacement is only possible in ax service centre.

Start-up of the SCX2e

Switching on the Device

The SCX2e does not have the capability to be directly powered by either AC or DC input. A power supply is always required to convert the provided (external) power into the 5VDC, which is required by the SCX2e. The power supply may be a fixed or removable part of the chassis/housing, where the SCX2e is mounted. As soon as the power supply unit is applied with external power, the agent-slot is powered and a plugged SCX2e will start.

After power is connected to either chassis or housing, the device boots its software automatically. No extra switch has to been activated. During the boot-process all internal components are roughly tested and the device is initialized. The last setup is restored; in case the unit starts the first time, it starts with the factory defaults.

The boot-process is indicated by the blinking ON-LED and takes about 2 minutes. At the end of this process the unit is fully operational. If there are any settings, which need special adoption, different to the default, the configuration can start now.

Power-Up Sequence

After providing power to the SCX2e, the device will power-up. The start-up will take several seconds, while internal SW is started and some tests are done to verify the SCX2e is not damaged and proper operation can be guaranteed.

The power-up sequence is indicated and can be monitored by special behaviour of the LEDs. After finishing the start-up, the LEDs will operate “normal” and indicate status and alarms of the unit, as written in this manual.

The special behaviour of the LEDs allow to user to

1. check, whether all LEDs or operating well and
2. see when the unit’s start-up is finished and the SCX2e is operational.

Configuration Access

After successful start-up process, the unit is ready for communication and configuration. A default setup is available as factory settings, but special settings can be done via several ways and methods. These will be depicted hereafter. All configuration settings are made by using the management I/Fs. For the system configuration you can choose one of the following configuration methods:

Local and Remote IP-Access

The SCX2e has two Ethernet I/Fs, which can be used for local and/or remote access. Local access means the direct connection of a Laptop and/or PC, while remote access is via LAN or WAN connection from somewhere else.

Remote access allows the user to communicate with the SCX2e and maintain the chassis via a long distance. The Combo-port can be used to hub the SCX2e into your local environment. The SCX2e can easily be integrated in umbrella management system or the Element Manager-function can be used, just as if the user is standing in front of the unit.

Daisy Chain

In the default configuration “Daisy Chain”, port MGMT1 is fully developed as Combo-Port, which is to offer the usage of either Copper (RJ45) or Fibre Optics (SFP). If a SFP is detected by the system, the copper port will automatically disabled (even when no FO signal is detected!). If no SFP is detected, the copper port is enabled and ready for operation. This combo-port MGMT1 is dedicated to be used for remote access (Q-mode). The second port (MGMT2) is split into two separate interfaces: The copper port (MGMT2a) is dedicated to be used a local access (F-mode) and the fibre part is the “Daisy Chain” to an optional next SCX2e. See Figure 1-2 for more details.

The default IP-settings for the 3 ports are:

- MGMT1 is configured as Q-interface (DHCP-client),
- MGMT2a is configured as F-interface (IP = 192.168.1.100/24) and
- MGMT2b is configured as “Daisy Chain”-interface and does forward all traffic coming from MGMT1.

Configuration Methods

Web Access

A Web-based GUI is available to configure and maintain the SCX2e locally and/or remote. All IP-based access methods can be used. For initial local configuration, please use port MGMT2a, as this is prepared for local access, by default.

1. Connect your PC / Laptop / LAN via any Ethernet cable (cross-over or straight) to port MGMT2a.
2. The SCX2e port MGMT2a is configured to act as an DHCP-server and will advertise the connected PC / Laptop an IP-address in the same subnet, as itself (192.168.1.100/24). To use this feature, the PC / Laptop has to be configured as DHCP client. (See Chapter 4, DHCP and Manual Address Assignment for details.)
3. Open your standard internet browser (e.g. Firefox) and enter in the address field **192.168.1.100**. The html-based GUI will allow easy configuration settings.

Secured Web Access

A secured web-access (https) is available. The access is the same as depicted above.

SSH Access

Secure Shell or SSH is a network protocol that provides secure communication between two computers. If SSH is used correctly, no eavesdropping or tampering with your data is possible, unless you are under attack by an immortal miscreant with extraordinarily powerful computers. Typically, SSH is used to securely log in to remote machines in order to execute commands.

All IP-based access methods can be used.

See Chapter 7, SSH and CLI, for details.

Telnet Access

Telnet access is not supported. Please use SSH-access for Command Line Access via TCP/IP.

SNMP Access

The SCX2e offers an on-board SNMP manager, which can be contacted by any available MIB-browser and/or SNMP manager. It supports SNMPv2c as well as SNMPv3 protocol, as defined by IETF.

As SNMP access is based on TCP/IP suite, the communication is possible via all ports.

The TCP-settings are the same as written above for the other ways of access. An easy and quick setup is implemented. See Chapter 6, SNMP and MIBs, for details.

Command Line Interface

The CLI is a basic way to do configuration and maintenance. It is very simple in style and requires more knowledge about the device. On the other hand, CLI is very well suited for scripting and replicating configuration. The CLI is depicted in Chapter 7, SSH and CLI.

Chapter 3
Hardware & Interfaces

This chapter provides information about the hardware of SCX2e - System Controller. This consist of block-diagram and a detailed description of all external interfaces and function indicators.

The SCX2e is a compact unit. All external connection points for control elements are accessible on the front panel. The indicator elements are also on the front panel.

Hardware Overview

Block-Diagram

The block-diagram shows the principal parts and functions of the SCX2e. The main blocks are shown and their logical connections are presented as lines in between.

The SCX2e can be divided into five functional blocks:

Table 3-1 *System Components*

	Component	Description
1a	Processor (Local Control Point LCP)	The SCX2e is based on a PowerQuick platform with an MPC8313E from Freescale. This CPU integrates a 32 bit power PC architecture and is clocked with 33MHz.
1b	Flash	The 64MByte non-volatile flash memory contains the program code for the operating functionality of the device as well as the system configuration. The software can be updated or added directly through the interfaces of the device. Therefore, it is not necessary to replace memory modules (for example EPROMs).
1c	SDRAM	The 128MByte main memory allows an high efficient operation of the CPU. The operating system (an embedded Linux distribution) will first be copied from the Flash memory to the SDRAM and then started from there.
1d	Alarm-Relay plus Alarm-LED	The alarm relay and LED show the status of the unit.

Table 3-1 System Components (continued)

	Component	Description
1e	Reset-Switch	If the IP-address has been forgotten or lost, this switch can be used to recall the default IP-addresses: MGMT Port1: 192.168.1.100 MGMT Port2: no default IP-address. MGMT-port2 waits for a DHCP-server to get its IP-address.
2a	NMS-Port1	10/100/1000BaseT plus 100BaseFX/1000Base-X port for local and remote access. NMS-port 1 can be grouped to one Combo-port. The bundling depends on the selected configuration.
2b	NMS-Port2	10/100/1000BaseT plus 100BaseFX/1000Base-X port for local and remote access. NMS-port 2 can be grouped to one Combo-port. The bundling depends on the selected configuration.
3	USB-Hub	25-Port USB-Hub to backplane. USB is the physical layer to the line-cards.
4a	DC/DC-Converter	The DC/DC converter is an own developed block, which generates all required voltage-levels out of the incoming 5V from backplane. It is temperature protected to prevent the device from damage.
4b	Backplane Connector	Via the backplane connector the SCX2e is connected to all line-cards, the Power-Supply and optional fan unit.
5	WDM-MUX	a WDM piggy-backed WDM system, working with 1310 and 1550nm wavelength. It is only available on the SCX2e-WDM.

SCX2e

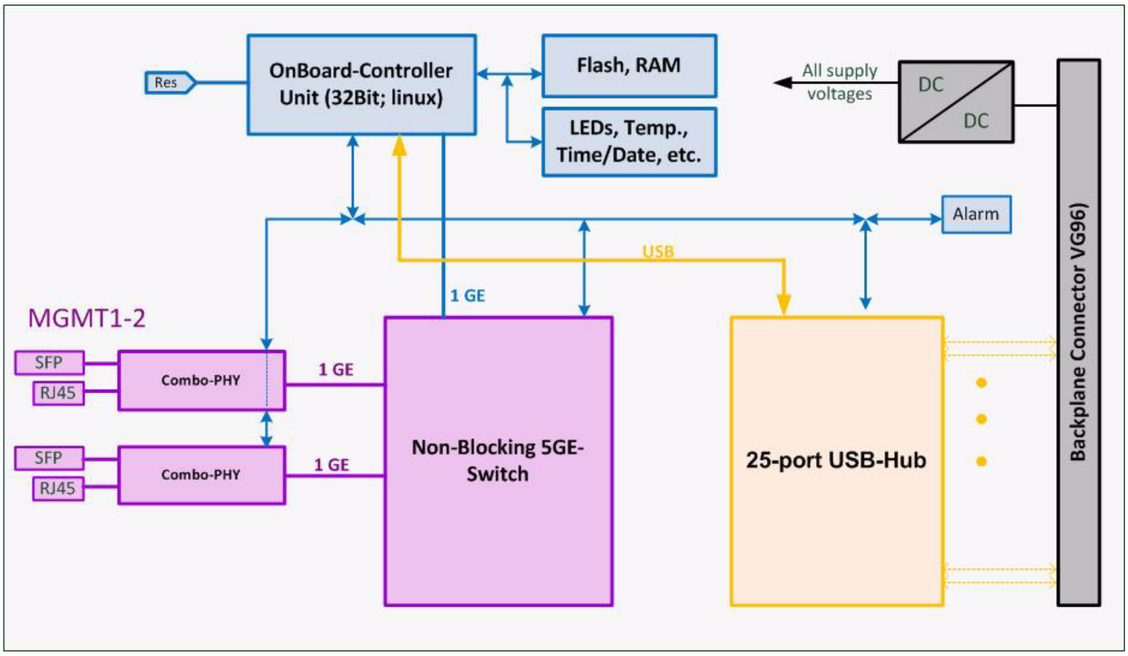


Figure 3-1 *SCX2e Block-Diagram*

Figure 3-1 gives an overview to the functional blocks. The four main blocks are coloured in different ways to distinguish them better from each other. The (blue) on-board controller runs a Linux-system and is the heart of the device.

The purple components build the external interfaces to access the device. Two (combo-) PHYs compose the physical interfaces and are switched in a little on-board LAN together with the controller. Each combo-port can be used either for Copper or Fibre Optic infrastructure. A third interface is available for the WDM-agent, only to achieve the communication to the peer unit. The two Ethernet MGMT ports use SFP/Copper combo-ports that can operate as fibre optic SFP-based interfaces or electrical RJ45 interfaces. The SFP/Copper combo-ports are auto detecting and can accommodate a wide range of Ethernet SFP transceivers, allowing service providers to seamless connect customers located at different distances from the device.

The communication between agent and line-cards inside the system, is done with USB. Up to 25 line-cards can communicate with the agent via USB. Though this large number is not necessary in all systems, larger applications can be build in future.

Towards the rack/system, the device does have a VG96 male connector. This connector is its internal interface and carries beside the USB and a lot of static lines also the power rail. A 5VDC input to the device is provided and all required voltages are generated on-board.

SCX2e-WDM

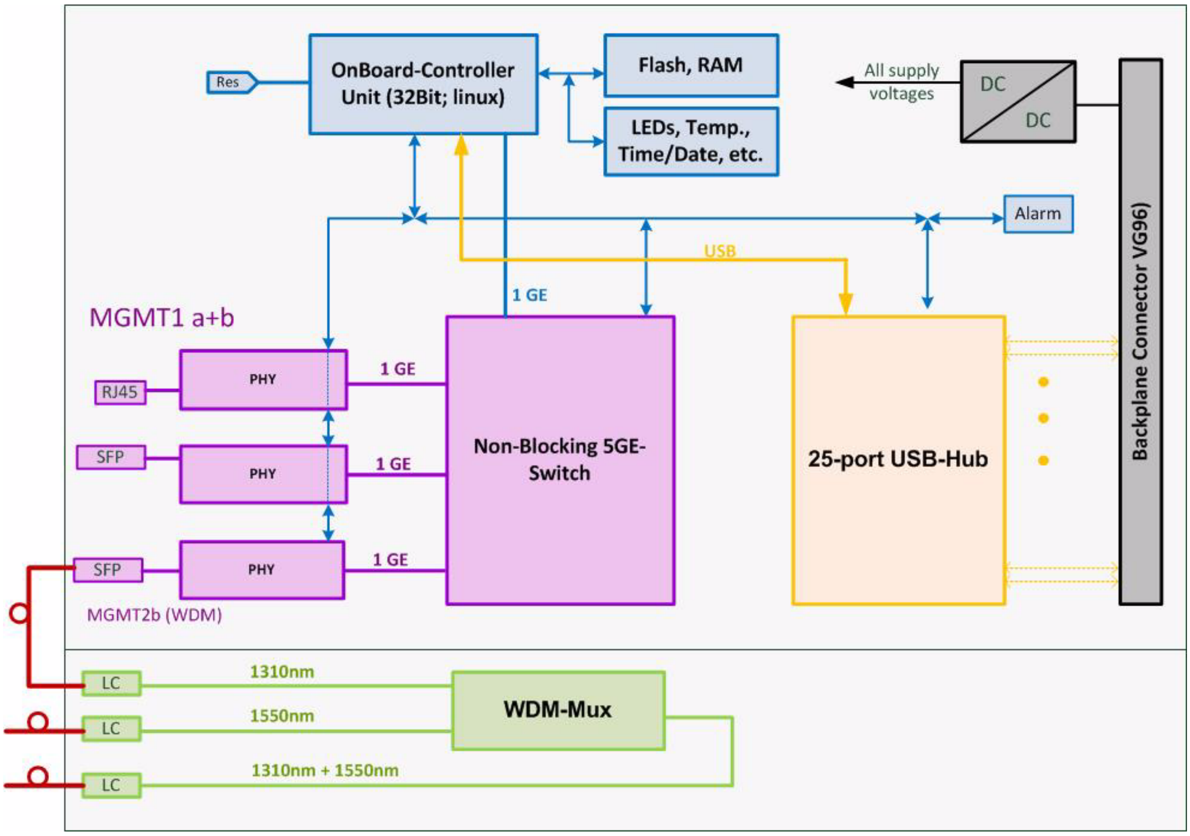


Figure 3-2 *SCX2e-WDM Block-Diagram*

The SCX2e-WDM has a slightly different assembly to achieve the requirements for this option. Instead of 2 combo-ports, it is assembled with 3 Ethernet interfaces, none of them as combo. 2x SFP port and 1x copper port is the choice here. In addition to these assembly variant, a complete WDM multiplexer is piggy-backed on the PCBA. The three connectors of the WDM-filter (1310nm, 1550nm, common) are accessible via LC couplers in the front-plate.

One of the two SFP ports (called MGMT2b) is intended to be connected to one of the WDM-lines (most likely the 1310nm link) via front-cable. It is NOT intended as a full-featured management interface, but shall be used to establish the communication link to the remote site via the WDM system.

SCX2e Front Panel

The SCX2e has full front access to all the connectors and status indicators which are required for the user. This makes it easy to install and changes in connection can be done without removing the unit from rack. The status indicators are all low-power LEDs, which are available in red, yellow and green.

The interface LEDs are labelled, so it is easy to use and understand the intent.

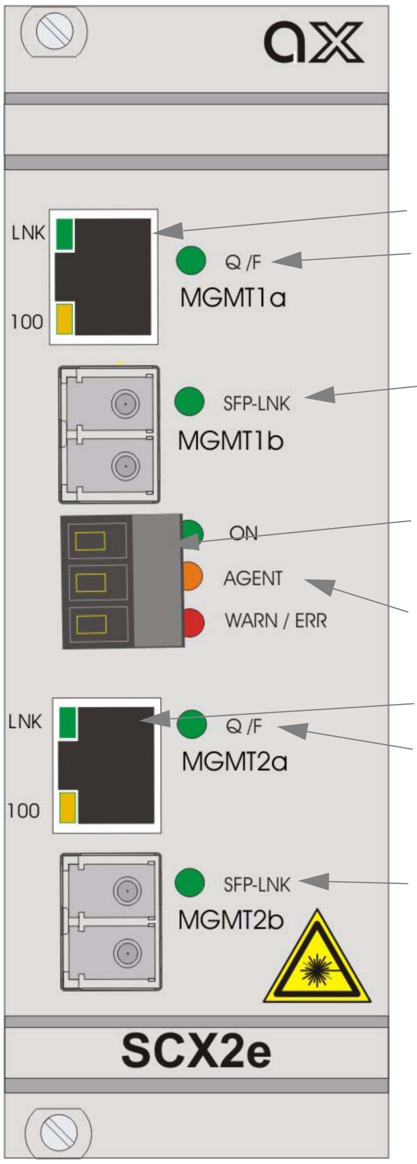
Two mounting screws at both ends of the front-plate are to fix the unit in rack or housing.

Front Views

SCX2e

Table 3-2 provides information on the connectors, indicators, and control elements of the SCX2e System Controller:

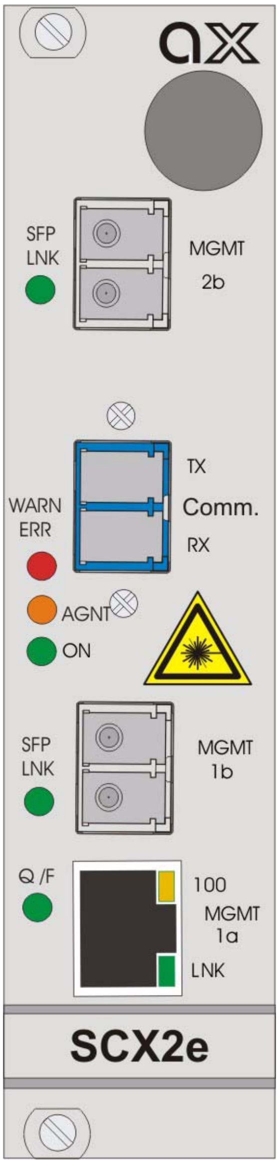
Table 3-2 *SCX2e Front View*

View	Product Number & Details
	Mounting screw in SRX. Handle w/o Label. 1x 10/100/1000BaseT MGMT Port, 2x integrated LEDs. 1x Q/F-mode LED for MGMT1. 1x 100FX/1000FX MGMT Port + 1x LINK-LED. 1x Alarm Connector. 1x ON-LED + 1x Agent-LED + 1x Alarm-LED. 1x 10/100/1000BaseT MGMT Port, 2x integrated LEDs. 1x Q/F-mode LED for MGMT1. 1x 100FX/1000FX MGMT Port + 1x LINK-LED. Handle with Label. Mounting screw in SRX.

SCX2e-WDM

Table 3-2 provides information on the connectors, indicators, and controls of the SCX2e System Controller:

Table 3-3 SCX2e Front View

View	Product Number & Details
	Mounting screw in SHX.
	Outlet of 2x WDM-Link
	1x SFP-Port (1310nm), connect to 1310nm-FO coming from WDM-outlet. 1x LINK-LED
	1x WDM-Port (1310+1550); common link to remote site.
	1x Alarm-LED + 1x ON-LED + 1x Agent-LED.
	1x SFP-Port (1550nm), connect to 1550nm-FO coming from WDM-outlet. 1x LINK-LED
	1x 10/100/1000BaseT MGMT Port, 2x integrated LEDs. 1x Q/F-mode LED for MGMT1.
	Handle with Label.
	Mounting screw in SHX.

Common Indicators

‘ON’ LED

The green ‘PWR’ LED indicates that the power supply of the SCX2e is available and the DC/DC converter is operating well.

‘AGENT’ LED

The yellow ‘AGENT’ LED indicates that the SCX2e is operated in main agent mode. For future purposes it is possible to change mode into sub-agent behaviour. This is not implemented yet. So for the time being, this LED will always be on.

In case the unit is configured to reset the IP-addresses to the defaults, the AGENT-LED will blink. Blinking of the AGENT-LED is the indicator for IP-reset. See Chapter 4**, Reset IP-Address to Default** for details.

‘WARN/ERR’ LED

The red ‘WARN/ERR’ LED indicates that there is a problem on the unit. Solid on is an error state, while blinking is an alarm state indicator.

NOTE: Only when the unit is in error state, the relay will be closed.

Management Interfaces (Ethernet)

The SCX2e does have four independent management interfaces, which are grouped to two bundles, called “MGMT 1” and “MGMT 2”. Both ports can be used as combo-ports, depending on the selected configuration. A combo-port can operate as fibre optic SFP-based interfaces or electrical RJ45 interfaces. The SFP/Copper combo-ports are auto-detecting the SFP option.

All SFP ports are compliant with [INF-8074i] and must be connected to SFP modules that are class 1 lasers and are compliant with [IEC 60825-1].The SFP-based interface will mostly be used for fibre optic data transmission. The port maximum speed of both ports is 1000Mbps.

Each copper-port consist of

- 1x RJ45-connector for 10/100/1000BaseT,
- 1x Speed-LED (in RJ45) to show speed of copper port,
- 1x LNK-LED (in RJ45) to show copper link and activity.
- 1x F/Q-LED to show the management/IP configuration of the port.

Each fibre-port consist of

- 1x SFP-slot for 100BaseFX or 1000Base-X,
- 1x LNK-LED for SFP-link and activity,

The combo-port can only use one of the two bonded interfaces: Either the copper port or the fibre (SFP-) port. If a SFP is detected by SCX2e, this will signalled by slowly blinking of the SFP Link-LED. In this case, the copper port may not be used!

WARNING: Do not place an SFP and a CAT-cable in parallel (at the same time) in one combo-port. This will lead to errors in transmission! This always true, even when one part of the combo is in “do-not-use” status.

Combo-ports can be configured by management to disable the auto-detection of SFP and they can be fix configured to support only fibre or only copper. In this case only the configured medium is supported and the other slice is not usable.

1000BaseTX (RJ45)

The SCX2e provides two copper Gigabit Ethernet interfaces as combo-ports. Separate indicators give information on the Link state (LNK) and activity (ACT) of the interface. The device negotiates the operating mode of the corresponding interface automatically with the remote station using Auto Negotiation (if activated). Half-duplex and full-duplex connections are supported. The data rate is either 10 Mbit/s, 100 Mbit/s or 1000 Mbit/s. The protocol is according to [IEEE 802.3]. Auto negotiation and auto crossover are supported.

NOTE: If the SCX2e detects an SFP in a combo-port, the adjacent copper-port will be disabled! If a SFP is detected the LNK-LED of the SFP will blink until the FO-link is established.

RJ45 Connector

The connector is a RJ45 plug with 2 LEDs, which indicate speed, link and activity. The pin-assignment of the RJ45 is as follows:

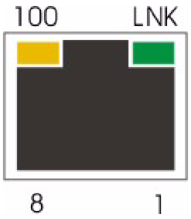
RJ45	Pin	Assignment
LED:	1	BI_DA+
	2	BI_DA-
	3	BI_DB+
	4	BI_DC+
	5	BI_DC-
	6	BI_DB-
	7	BI_DD+
	8	BI_DD-

Figure 3-3 *Ethernet-Pinout R45 Connector*

The integrated LEds in the RJ45 connector, do have the following behaviour:

- The yellow LED (’100’) indicates the speed of the link:
  - 1x blink = 10Mbps
  - 2x blink = 100Mbps

    - 3x blink = 1000Mbps
- The green LED ('LNK') indicates, when the link is established and packets are transferred.

Auto-Cross-Over

The device is able to recognize

- a polarity inversion of the receiving signals (RD+ <--> RD-)
- a crossover of transmitting/receiving signals (RD+/RD- <--> TD+/TD-)

and corrects it automatically ensuring that the operation continues smoothly.
This allows the usage of 1:1 cables in any case.

CAUTION: For access it is recommended to use twisted-pair cables of the category 5 and an impedance value of 100 Ω. The maximum cable length is 10 metres. Using cables of lower quality or different impedances may result in a restriction of the maximum cable length. In addition the employment of unshielded cables can have negative effect on the reliability of the data transmission.

1000Base-X (SFP)

The SCX2e provides two fibre Ethernet interfaces as combo-ports. Both ports can be equipped with an 100BaseFX or an 1000Base-X module according the SFP industry standard.

For each interface one indicator gives information on the link state and activity (LNK).

- The green LED ('LNK') indicate(s) that the optical link is established.
- If a SFP is detected in the SFP-slot and there is no link established, yet, the LNK-LED is blinking. This is to indicate that the copper port is disabled, as the SFP is plugged.

Standards

Table 3-4 *Ethernet Standards*

Item	Values
Standards:	IEEE 802.3, 801.1 p&Q
Data rate:	Copper Port: 10Mbit/s, 100Mbit/s or 1000Mbit/s auto negotiation, full- or half-duplex, bandwidth limitation Fibre Port: 1000Mbit/s auto negotiation, full- or half-duplex, bandwidth limitation
MTU	10240 Bytes (also selectable 1522 or 2048 Bytes)
Flow Control:	IEEE 802.3x, PAUSE frames

WDM-Filter

Only available on the SCX2e-WDM!

A passive optical filter is part of the SCX2e-WDM system. Optical filter are passive multiplexer modules which split or combine the light of several wavelength.

The used filter combines the light generated by two individual channel modules (SFP or XFP) and performs the actual multiplex function before sending the data onto the link fibre. there are only two wavelength supported by the filter:

- 1310nm - intended for the management link,
- 1550nm - intended for the user’s payload.

At the other end of the fibber cable an inverse filter de-multiplexes the received 'rainbow' into the two individual channels. The used filter module combines mux and demux in one compact package. An identical filter module is used at each of the link.

The three fibre optic links of the WDM filter are labelled, to make the installation easy:

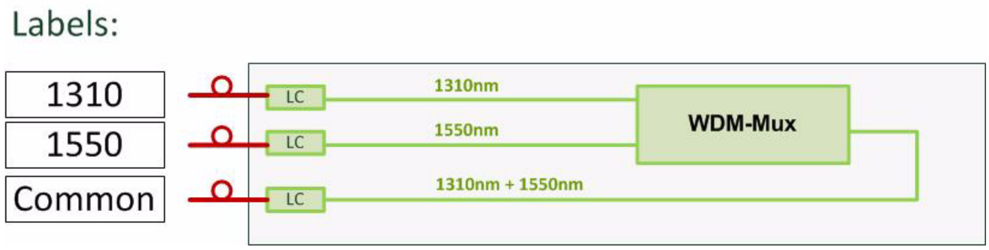


Figure 3-4 *WDM-Filter Labels*

Alarm Connector

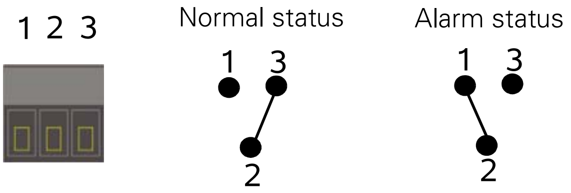
An alarm connector is used in order to indicate an alarm of the system.

NOTE: Not available on the SCX2e-WDM.

Normally a line, fan and/or power failure sets the system to alarm status. Please check manual of installed devices, which additional events can cause an alarm.

Table 3-5 shows the alarm connector settings.

Table 3-5 *Pin Assignment Alarm Connector*



Pin:	Connect to:
1	Normally open "NO"
2	Centre contact
3	Normally closed "NC"

NOTE: The contact is galvanic separated. The contact rating allows a resistive load with max. 1 A, 30 V AC/DC.

LEDs

Several LEDs show the (operational) status of the device. During start-up of the device the LED have different meaning than during normal operation (see “LED Start-Up” on page 2-4). In this chapter, the behaviour after successful start-up is depicted.

ON & ALM

The ON-LED is used for power-supply indication, while the ALM-LED shows the alarm status of the device. After Power-On of the device, both LEDs will be on.

ON-LED	**Display states of the LED:**	
○	off	No supply voltage.
●	on	Supply voltage available.
✦	flashing	Power available, device did not start (yet).

ALM-LED	**Display states of the LED:**	
○	off	Neither error nor warning detected.
🔴	on	Device has at least one error detected.
✶	blinking 1.5 Hz	Device has at least one warning (and no error) detected.

Agent-LED	**Display states of the LED:**	
○	off	Device defect.
🟡	on	Device operates normal.

Ethernet

The device does have 2 management ports, which are used for Ethernet based access to the device. The two ports are RJ45 with integrated 2 LEDs each. The label of the 2 LEDs are 100 and LNK. The “REMOTE”-port does have an additional LED (Q/F), which indicates the status of IP-address assignment to this port.

100-LEDs	**Display states of the LED:**	
○	off	The Ethernet port speed is 10Mbps (10BaseT).
🟡	on	The Ethernet port speed is 100Mbps (100BaseT).

LNK-LEDs	**Display states of the LED:**	
○	off	No Ethernet link detected.

●	on	Ethernet link is established, and no traffic is ongoing.
✦	flashing	Ethernet link is established, and traffic is transferred. The LNK-LED blinks for ingressing or egressing packets.
SFP-LNK-LEDs	**Display states of the LED:**	
○	off	Neither SFP nor Fibre-Ethernet link detected.
✶	blinking 1.5Hz	SFP in slot detected, but no Fibre-Ethernet link is established.
●	on	Fibre-Ethernet link is established, and no traffic is ongoing.
✦	flashing	Ethernet link is established, and traffic is transferred. The LNK-LED blinks for ingressing or egressing packets.
Q/F-LED	**Display states of the LED:**	
○	off	Remote port is disabled or is acting as F-interface (DHCP-server is activated on this port).
●	on	“REMOTE” port is operational and it has at least one valid IP-address (IPv4 or IPv6).
✶	blinking 1.5Hz	“REMOTE” port is searching an DHCP-server and waits for IP-address assignment.

Reset Switch

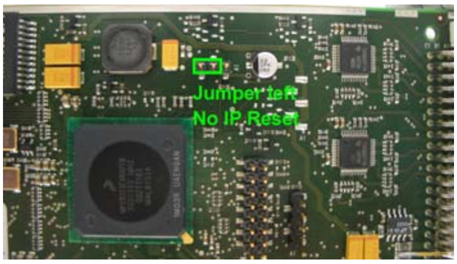
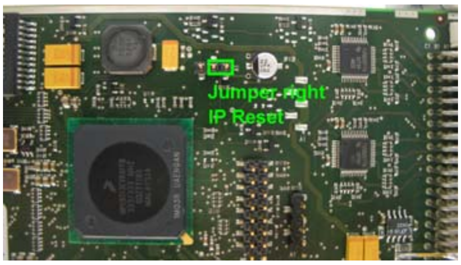
A small reset switch is placed on the top side of the unit. This switch is dedicated to reset the IP-address(es) of the device to the factory defaults. In case you have lost the IP-address of the unit, please reset the IP-address to a known value to re-start the communication and enable further configuration. When the switch is closed, the AGENT-LED is blinking to indicate this special status in which the device uses its IP-defaults.

The default IP-address of the MGMT port 1 is <empty> (DHCP-client).

The default IP-address of the MGMT port 2 is 192.168.**1**.100/24.

How to reset the addresses will be depicted in all details in Chapter 4**, Reset IP-Address to Default**.

Table 3-6 *IP-Reset Setting*

Normal Operation	IP-Reset
	

Chapter 4
Functionality

Agent

The task of the SCX2e as an agent in the provider's network is to be provide a single management interface for configuration and maintenance of the ax system.

The SCX2e collects all information of the ax MSP (Multi Service Platform) and gives access to it by different possible protocols, which are used as northbound interface. In the same way, the SCX2e allows access to all managed objects and their change and supervision.

An agent does normally do not send any information by default, but only reacts upon request of the management system. The SCX2e can be configured to inform the management system spontaneous by sending traps to several receivers so changes and alarms can be recognized very quick.

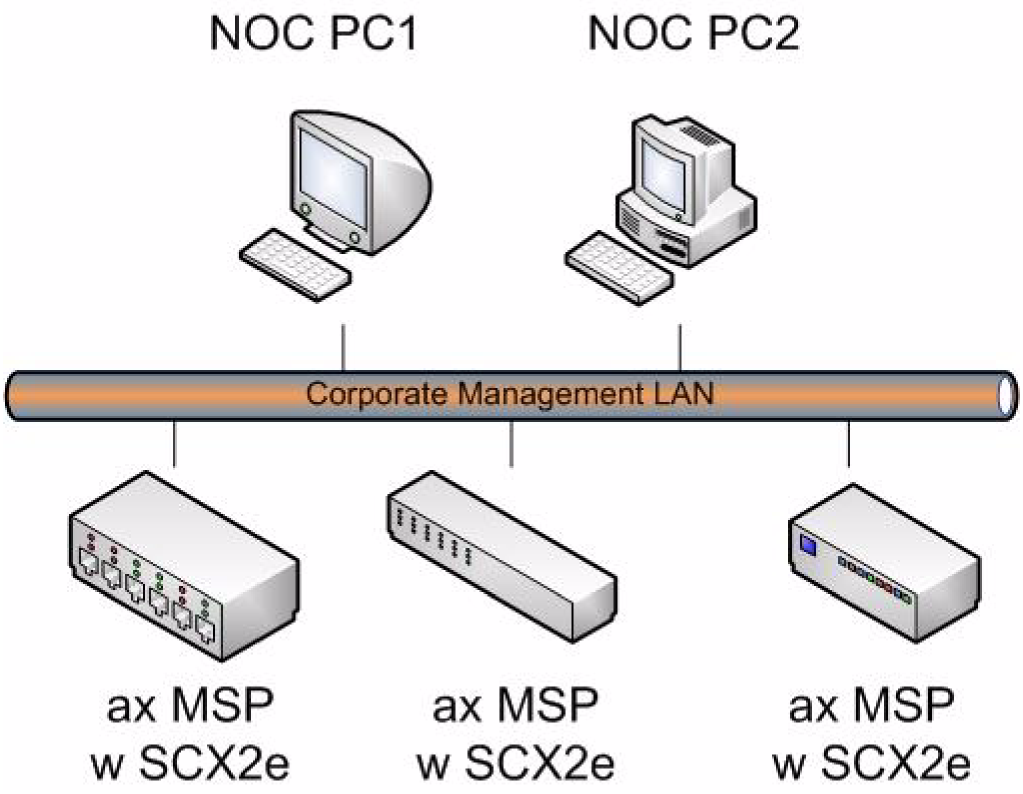


Figure 4-1 *Agent Architecture*

SW-Update

The SCX2e is not only an agent but offers also the possibility to act as a hub for SW-update files. It can store several different SW-files for line-cards (LC) and the administrator can choose time and version of a new file to be installed.

The SCX2e keeps track on the versions and which file is valid for which LC so it is very easy to keep control. New files can easily uploaded to the file-storage of SCX2e via HTTP, SFTP and TFTP.

User & Access Administration

Access-Options to the SCX2e

The SCX2e offers several physical ways to get access to the device together with different options to authenticate and authorize. In total, one can differentiate four protocol stacks, which are supported. These four protocols to get management access to the SCX2e are

- HTTP (Web-based GUI via TCP/IP)
  - See Chapter 5, SCX2e Web-GUI, and [axRefGuideWebGUI_SCX2e].
- HTTPS (Secured Web-based GUI via TCP/IP)
  - See Chapter 5, SCX2e Web-GUI, and [axRefGuideWebGUI_SCX2e].
- SNMP (including traps)
  - SNMPv2c and SNMPv3 are supported.
  - See Chapter 6, SNMP and MIBs.
- SSH-CLI (command-line-interface via secure shell)
  - See Chapter 7, SSH and CLI, and [axRefGuideCLI_SCX2e].

All four access-options can be disabled individually, but at least one of them must be active.

NOTE: If the last of the four access-options shall be disabled, the SCX2e will deny to accept this.

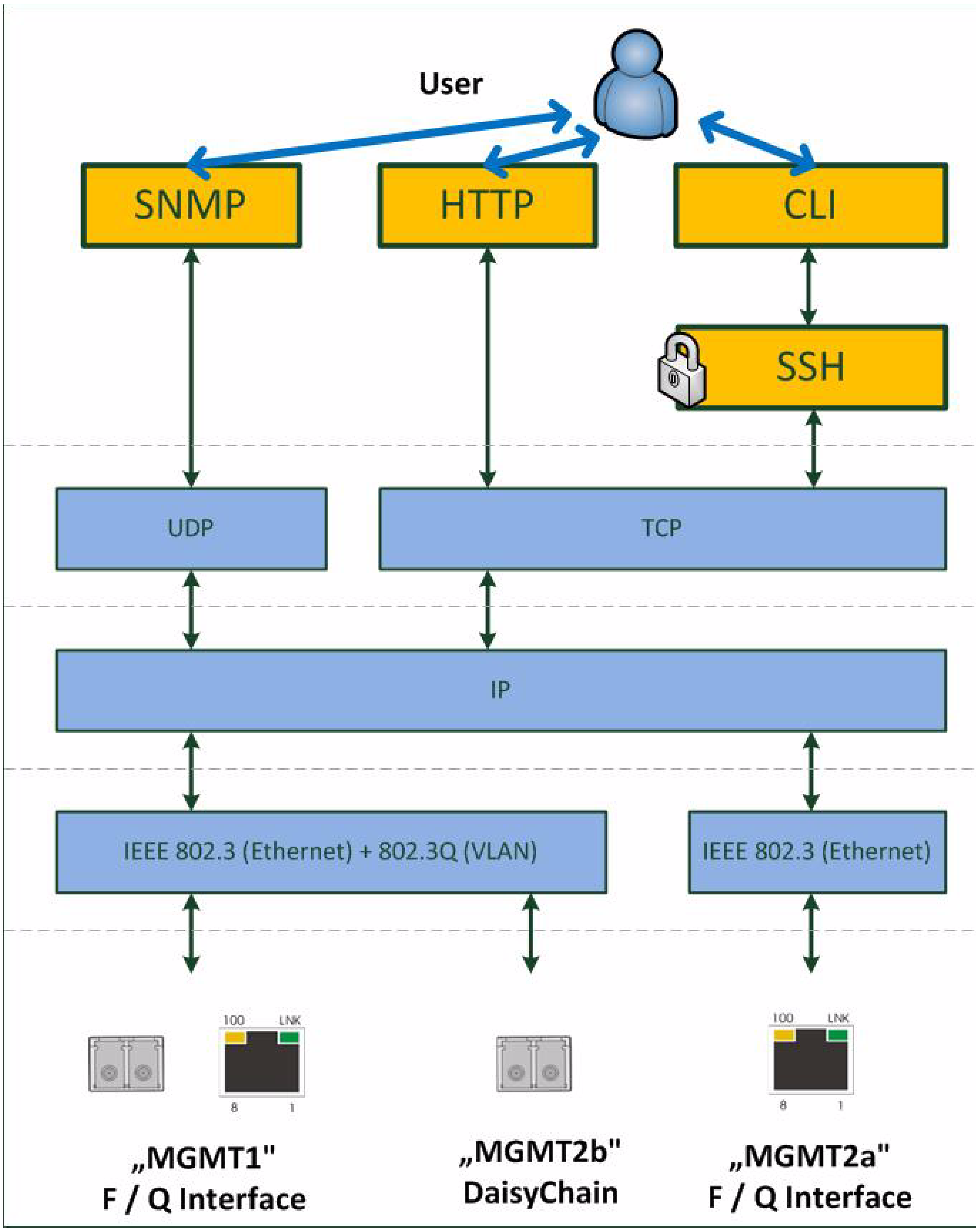


***Figure 4-2** Management Protocol Stack*

Figure 4-2 shows the protocol stack for the management access to the SCX2e and the attestant physical interfaces to be used.

SSH-Access

The SSH-access offers a secure connection to the device. Keys and passwords might be used to make the communication safe and secure. If required by the user, the SSH access can be disabled at all, to avoid illegal access to the device. In factory default, the SSH access is enabled.

Details about the usage, configurations and options of the SSH-access is written in Chapter 7, “SSH and CLI”.

User Administration

All the different access-options to the SCX2e are protected by user-name and password. Several users can be configured on the SCX2e and stored locally, or one can use a (central) server, which stores the different users passwords and levels. Each user can have one of three different levels of authority:

- admin,
- user,
- guest.

A new user can be created on the SCX2e locally with access-level, user-name and password. Or it can be stored on a NAS (Network Access Server). When a NAS is used, the protocol TACACS+ is used.

The administrator of the SCX2e can decide, whether the locally stored users, the TACACS-users or both shall be accepted and access granted. Any not successful attempt to login to the device is stored in the log-file and a trap can be configured to inform higher level management system about this.

Locally Stored Users

Locally stored users can be created, modified and deleted by the administrator. The number of locally stored users is limited to 99. If a locally stored user shall be inactive, it must be deleted.

NOTE: After the creation of a new user together with password, only the user itself can change its password. If the password was lost, the user must be deleted and re-created again.

When delivered, the SCX2e does have one locally stored user:

user-name: ’admin’

password: ’private’

WARNING: It is highly recommended to change the password of ’admin’ due to security reason!

NOTE: The user ’admin’ can never be deleted. Only the password of ’admin’ can be changed.

Rules for Usernames

When a new user has to added to the onboard user-list, some simple rules must be considered:

- The (new) user name must consist of at least 3 characters.
- The following characters are allowed: ‘0-9’, ‘a-z’, ‘A-Z’, ‘_’, ’.’, ’-’.

Rules for Passwords

The password given to a user or other usage must reach a certain level of “password strength” to protect the system from hackers. The strength of a password is a function of length, complexity, and unpredictability and this is verified by several security rules. If a new password does not fulfil this rules, it will be not accepted by the SCX2e. The rules are as follows:

- Minimum password length is 3 characters (, maximum password length is 32 characters),
- Character set is 7-Bit ASCII, allowed characters:
  - Capital letters: A...Z,
  - Lower case characters: a...z,
  - Digits: 0...9,
  - additional characters: 0x2D (-), 0x2E (.), 0x5F (_)
- The password may contain any of these characters.

NOTE: It is allowed to have the user-name as part of the password (forwards and backwards, not case sensitive!). BUT the system will remove this string from the password before it is verified.

- E.g. the user-name is “weakuser”. Then a password “12weakUser!” would lead to strength-verification of “12!”. The password would be too weak and not accepted!
- The same user-name in combination with password “12weakuser!_ButStrongPassword” would be ok, as the strength-verification is done on the reduced password “12!_ButStrongPassword” and this fulfils the requirements for a strong password.

Auto-Logout

At the end of a management session it is highly recommended to stop the connection and logout from the unit. This is a safety requirement to make sure nobody else can use the current login without authorization. Nevertheless it can happen that this security demand is not observed, due to:

- Problems of your Computer,
- Problems in the network,
- Laxness of user,
- etc.

To make sure, a forgotten or incomplete logout, or a still open connection is closed there are some features to enforce auto-logout.

Time-Based Auto-Logout

First, there is an auto-logout time, which will terminate each CLI, SSH and Web-GUI session after “No activity”. This auto-logout time can be specified. It defines the time of inactivity, which causes an automatic logout. The specified time-interval is valid for all logins, and each login does have its “own” timer. A “login” is the combination of user and access (e.g. user “admin” via “SSH” or user “test” via “http”).

Note: If auto-logout-time is defined to zero, the auto-logout is disabled for all logins.

The detection of activity is different for the access options.

CLI:

- For the CLI activity is the <enter> command which sends a new instruction to the device.

Web-Page:

- For the Web-GUI, activity is changing a variable-value, moving to a new page or reload of the existing page.
- A second time-based logout is a java-script for web-GUI. If for 15 seconds the browser does not reply a “hello”-message from the device, it is assumed the browser or browser-tab was terminated and a log-out will happen.

Protocol-Based Auto-Logout

A CLI-over-SSH session will be automatically terminated, when the SSH-link is closed.

Management Port Configuration

The SCX2e can be managed via different protocols using the TCP/IP stack (see Figure 4-2) across the management interfaces “MGMT 1" and “MGMT 2a”.

Both ports need a valid IP configuration (host address) and the physical layer (“Port Settings” of both can be configured.

Port Settings

The port settings of the management ports are the physical setup and status (Layer 1). The ports can be enabled and the speed and duplex capability can be defined. In standard networks it will be the best to keep the autonegotiation feature of the port, but it might be necessary to adopt this. Autonegotiation options are depicted in chapter “Auto Negotiation” on page 4-13.

The name of the port can be adopted to make it better readable and more meaningful for user. This name will be used in traps, which can be enabled to announce changes in the link state of the ports.

Some entries show the status of the port and some high-level counters to see whether the port is operational and working or not.

If the MAC address of the port is needed for other application, one find it here as an read-only entry.

NOTE: The MAC address of a port can not be changed by user.

IP-Addressing

Both ports need to be configured with a valid host-address before usage is possible. Defaults are stored on the device, but these will seldom fit into the given environment.

Both ports do support manual address assignment as well as the dynamic host configuration protocol DHCP.

NOTE: The host address of the two ports MUST be in different IP-subnets, otherwise the dive will have unpredictable behaviour and IP-based communication will not work correctly.

The Default GW and the TTL-value (time-to-live) is a global settings, valid for both ports. So this setting is not related to one of the two ports, but a common part which can be configured globally.

Management Port “MGMT1” and “MGMT2a”

The out-of-band management ports can be used in local (F-interface mode) and remote (Q-interface mode), which has influence on the IP-address scheme. The different behaviour are depicted in “F- and Q-Interface” on page 4-8.

To integrate SCX2e into a larger network management environment, it can be configured to use VLAN-tagging on the port. This makes only sense, when it is operated in Q-mode, as the F-mode is for real local access. The VLAN-tagging can be enabled on demand and all valid VLAN-IDs can be used. This VLAN-ID is really separated on the device and does never interfere with other VLAN-IDs configured, e.g. for the payload or in-band traffic.

When the port is configured to operate as DHCP-client, a DHCP-server will be searched at the beginning. The server’s address and the resulting settings can be verified on the unit.

Daisy Chain Configuration

MGMT1 (Combo):

- Default Mode: Q-interface
- Default IP-address and mask: <empty>
- Default VLAN-ID: 4094
- Other Defaults: Act as DHCP-Client

MGMT2b (SFP):

- Default Mode: Daisy Chain
- Default IP-address and mask: always same setting as MGMT1!

MGMT2a (RJ45):

- Default Mode: F-interface
- Default IP-address: 192.168.**1**.100/24
- Other Defaults: Act as DHCP-Server

DHCP and Manual Address Assignment

The IP-address of the two management ports can be assigned by an DHCP-server or manually. If an DHCP-server is used, it must be connected to the interface. If no DHCP-server is available for this interface (or just not reachable), the unit starts with the Default IP-address of the interface (see above).

Note: We have sometimes seen problems with DHCP communication over some available USB-to-Ethernet adaptors. This problem is not related to SCX2e, but the implementation of these adaptors. Best results is reached with onboard Ethernet-ports.

After assignment of the management IP-address (via DHCP or manually) the SCX2e is reachable within the existing IP-network. It makes no difference whether the communication uses the out-of-band or in-band interface.

F- and Q-Interface

F- and Q-interface are two different behaviours of a management interface port.

The behaviour of an interface configured as “F-interface”, is defined by ITU for local access. The F-interface implementation of arcutronix does incorporate a DHCP-server, which makes it very easy to connect your laptop via Ethernet-cable. In your standard laptop configuration, it will get a valid IP-address from the SCX2e and the IP connection can be used.

NOTE: The DHCP-server can only assign one(!) IP-address, so it makes no sense to connect a complete LAN to this port, using the SCX2e as DHCP-server for the LAN!

If the interface shall be used for remote access, the proper configuration will be “Q-interface”. In Q-interface mode, the SCX2e will act as a DHCP-client and gets an IP-address via the connected network (as long as a DHCP-server is setup somewhere in the network).

The Q/F-LED at each management port does indicate the mode. When the LED lit, the port is in Q-mode, when it is off it works in F-mode. When the port is acting as DHCP-client, the Q/F-LED is blinking, as long as there is no valid IP-address assigned.

DNS-Support

SCX2e does support name service (DNS) to support easy access to the device. In f-interface mode, one can reach the SCX2e by using “ax-<device-type>” instead of the IP-address. For the SCX2e it would be **ax-**SCX2e.

An example is shown below. The SCX2e has been assigned the IP-address **192.10.4.10**. A ping-command will result in the following:

```
C:\> ping ax-SCX2e

Ping ax-SCX2e [192.10.4.10] with 32 bytes data:

Reply from 192.10.4.10: Bytes=32 Time<1ms TTL=128
Reply from 192.10.4.10: Bytes=32 Time<1ms TTL=128
Reply from 192.10.4.10: Bytes=32 Time<1ms TTL=128
Reply from 192.10.4.10: Bytes=32 Time<1ms TTL=128

Ping-Statistics for 192.10.4.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% Loss),

C:\>
```

Reset IP-Address to Default

In case the given IP-address of the SCX2e is lost or forgotten, there is a way to reset it to the factory default, so communication can start again and a new IP-address can be assigned. The reset will stop the operation of the SCX2e, but as communication is anyhow not longer possible, this is not relevant. The services (of the line-cards) are NOT effected by the reset!

In the following the 4 steps to reset the IP-address to defaults will be shown. The defaults are:

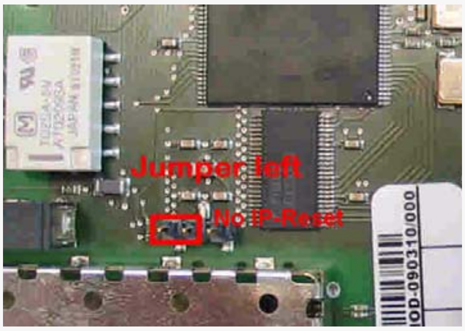
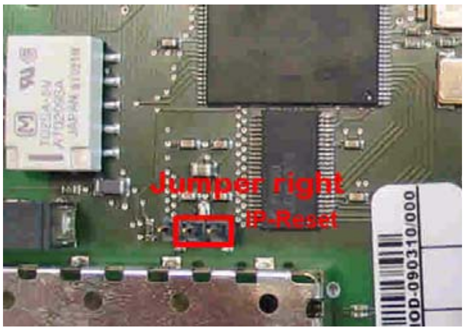
The default IP-address of the MGMT port 1 is 192.168.**1**.100/24.

The default IP-address of the MGMT port 2 is <empty>.

1. Place Reset-Jumper

Remove the SCX2e from the chassis and place the jumper on the reset-switch as shown:

Table 4-1 *IP-Reset Setting*

Normal Operation	IP-Reset
	

2. Start again and Login with Default IP-address

Plug the unit back to the chassis and let it start. After successful boot-process, the AGENT-LED will blink permanent. This is the indicator for IP-RESET-mode.

Now you can connect to the unit with the default IP-addresses and log onto the device just as before.

After login, change IP-settings of the ports as required. The new settings are stored automatically.

NOTE: After changing the IP-addresses to the new values, you might loose contact. In this case you have to re-establish communication with the new settings, if further settings are required to do.

3. Remove Reset-Jumper and Start again

To leave the IP-RESET-mode remove the unit again and remove the reset-jumper. After restart, the new settings are valid.

NOTE: If you do not remove the Reset-jumper, the SCX2e will have the default IP-addresses again after any reboot! You can see the IP-RESET-mode, when the AGENT-LED is blinking.

Firmware-Update

It might be necessary to update the software (firmware) on the SCX2e. In this case the new firmware can be uploaded to the device via several ways:

- HTTP, HTTPS, TFTP and SFTP

Only SFTP is a secured way to upload the new firmware and is highly recommended to be used. See chapter “File-Transfer to/from Servers and via HTTP(S)” about the configuration and usage of the different protocols.

The update-file has the extension “*.upx” and is a special arcutronix file format. It is secured by a checksum and other mechanism to make sure only correct files will be accepted for firmware update. If the file transfer did not work properly or any other damage of the update-file is discovered, the new file will not be accepted for update.

NOTE: A corrupted file can be uploaded to the SCX2e, but it will not be used for update. The security check can only be done, when the file is on the device.

After successful upload, one can start the proper update. When update (not upload) is started, the unit will do a reset right after successful installation of the new firmware. If the update process did not work properly, or the new firmware does not start correct, the old FW-version will be used instead. The old version will be stored on the device till the next update process.

File-Transfer to/from Servers and via HTTP(S)

The SCX2e can upload and download different files for internal usage or external storage:

- New Firmware-Update file to be used on the device to offer new features:
  - Files need to be loaded onto the device.
- Actual configuration can be stored externally for backup or further usage:
  - Files need to be stored on a server.
- Profile configuration can be installed for quick setup of the device:
  - Files need to be loaded onto the device:
- Log-files can be stored externally to be analysed:
  - Files need to be stored on a server.
- SSH-keys can be stored on the device for proper authentication:
  - Files need to be loaded onto the device.

For these storage- and loading-operation of files three ways are foreseen in the SCX2e:

- HTTP, HTTPS, TFTP and SFTP

NOTE: Only SFTP is a secured way for file transfer and it is highly recommended to use SFTP.

The different ways of file-transfer to diverse servers and the direction of up- and download in shown in the following picture:

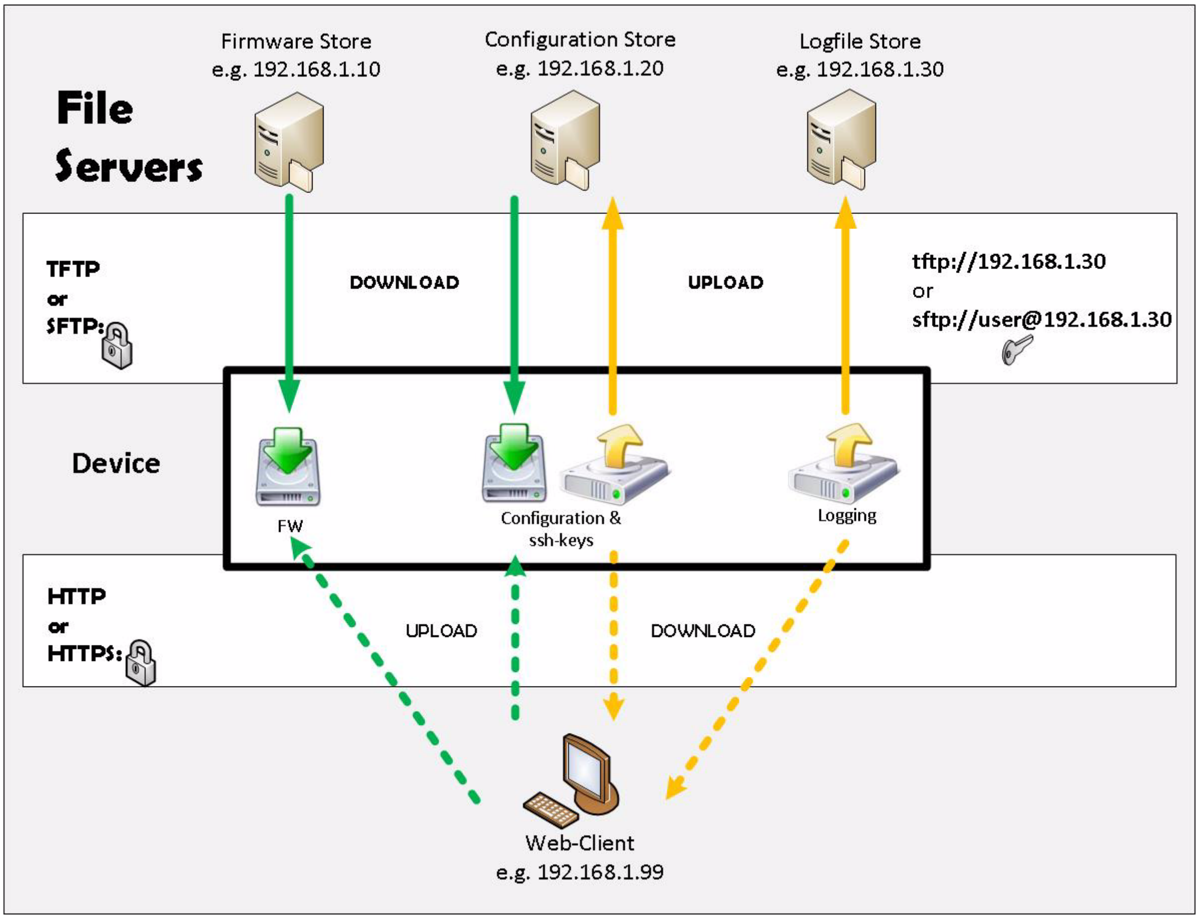


Figure 4-3 *File-Transfer*

While SFTP and TFTP are providing download from the server to the device, the http protocol is uploading to the device. The same opposed naming applies for the transferring files from the SCX2e to a server.

SFTP and TFTP

Three servers can be configured for SFTP or TFTP file-transfer:

1. Firmware-Store to download new firmware
2. Configuration Store to download config-files and SSH-keys and to upload config-files
3. Logfile Store to upload log-files.

The 3 servers can use the same IP-address, but for security reasons the servers can be divided to different physical locations and use different rights of access. For each server it can be defined, whether it speaks SFTP or TFTP and the proper user settings must be made before usage.

If no valid server settings are provided, no SFTP and TFTP access is possible.

Note: If the usage of SFTP or TFTP must be disabled, just avoid valid settings.

HTTP and HTTPS

The usage of HTTP and HTTPS for file-transfer is a very easy way to move files with the help of your browser. In the http-case of file-transfer, the SCX2e is acting as the (web-)server and the user at the terminal can upload and download files to it.

HTTP- and/or HTTPS-file transfer can be disabled entirely due to security reasons.

NOTE: The usage of http (https) is only possible via a http- (https-) session and not available for SSH or CLI applications!

WARNING: When the file-dialogue windows is opened for file-selection or storage, a security feature is implemented to avoid uncontrolled usage: After a time-frame of 5 minutes with opened file-dialogue, the user will be logout from the system automatically.

Miscellaneous Features

Auto Negotiation

Modern Ethernet interfaces support a mechanism called Auto-negotiation to allow connection of ports with different capabilities. During the auto-negotiation process

- Speed (10, 100 or 1000Mbps),
- Duplex mode (full duplex or half duplex),
- Flow Control capabilities and
- Clock Settings

are defined for the established link.

Speed and Duplex

Auto-negotiation is part of [IEEE 802.3], the Ethernet standard. It was first defined in 1995 as IEEE 802.3u and was an optional implementation. Unfortunately at this time the standard gave partly space for interpretation and so different implementation in older equipment can be found. In 1998 the debatable portions were eliminated and a year later the standard was extended for Gigabit-Ethernet.

In the market, there is still a lot of the older equipment, where auto-negotiation was not clear defined, so there may occur problems when devices try to do auto-negotiation. So some devices do still expect to “talk” auto-neg, even when the port’s speed and duplex mode are strictly defined by the user. For this reason, SCX2e supports to enable and/or disable the auto-neg communication, when the port’s speed or duplex mode is not really matter of negotiation but fixed by the user.

Please see table below for the possible settings and the resulting behaviour.

Table 4-2 *Settings Auto-Negotiation*

Setting (Port Speed)	Result		
	Speed	**Duplex**	**Remark**
Automatic	10, 100 or 1000 Mbps [i]	Full or Half Duplex [ii]	Full Auto-neg takes place; no limitations are given. The variable “Autonegotiation” is not changeable, but always “ON”.
10 Half Duplex	10 Mbps	Half Duplex	Auto-neg communication with peer can be enabled via the “Autonegotiation” variable.
10 Full Duplex	10 Mbps	Full Duplex	Auto-neg communication with peer can be enabled via the “Autonegotiation” variable.
100 Half Duplex	100 Mbps	Half Duplex	Auto-neg communication with peer can be enabled via the “Autonegotiation” variable.
100 Full Duplex	100 Mbps	Full Duplex	Auto-neg communication with peer can be enabled via the “Autonegotiation” variable.

Table 4-2 Settings Auto-Negotiation (continued)

Setting (Port Speed)	Result		
	Speed	Duplex	Remark
1000 Half Duplex [ii]	1000 Mbps	Half Duplex	Auto-neg communication with peer can be enabled via the “Autonegotiation” variable.
1000 Full Duplex [ii]	1000 Mbps	Full Duplex	Auto-neg communication with peer can be enabled via the “Autonegotiation” variable.

i. Depending on ports capability and auto-negotiation result.

ii. Depending on auto-negotiation result. All SCX2e ports do support full duplex mode.

Alarm Management

The SCX2e does have an outstanding alarm management, which allows users to get a quick overview of the current device status, but also to get detailed information about individual alarm states. The alarms are grouped by function or hardware component, each group can be configured and acknowledged as group. Or one can navigate into the groups and configure each alarm in detail for the personal preferences.

Alarm Types

In general terms, an alarm monitors the value of a certain quantity for exceptional values. If such an exceptional value is detected, the alarm condition is said to be active. Depending on the configuration of the alarm, this may cause the alarm to become active as well.

There are two fundamentally different types of quantities that can be monitored by alarms. The first one are quantities that have a well-know set of discrete states, some of which may represent exceptional values. An example is the link state of an ethernet interface which may have the states “Link Up”, “Link Down”, and “Port Disabled”. Here “Link Down” represents the exceptional value that causes the alarm condition to become active. Alarms that monitor these discrete-state quantities are called **digital alarms**.

The second type of quantities represent physical quantities that usually vary continuously. Here, exceptional values are defined in terms of thresholds that limit the acceptable operational range for the physical quantity. Depending on the quantity being monitored, the device checks upper and/or lower bounds for the acceptable operational range and allows to define the corresponding threshold values. An example of this type of variables is the device temperature, for which an acceptable operational range may be defined as -20°C … 60°C. Alarms that monitor these continuously varying quantities are called **analogue alarms**.

NOTE: For analogue alarms it is possible to define the warning level at a higher value than the error level. E.g. for the temperature is possible to define the warning @60°C and the error @55°C. This is not forbidden by the system, as there might be customer's reason to do so.

Alarm States

The state of each alarm is determined by several factors.

The first one is the **alarm condition**. The alarm condition can be unavailable which means that the quantity being monitored is not well-defined, which may occur due to the current device configuration. In case of the Ethernet interface example above, the link status is not defined if the Ethernet port is disabled by the administrator. The alarm condition can also be active or inactive, which indicates that the monitored quantity has an exceptional value or indicates normal operational conditions, respectively.

The second factor that affects the alarm state is the alarm configuration. It may affect the state of the alarm when the alarm condition becomes active, but it may also define parameters for detecting the alarm condition:

- Alarm configuration can force the alarm condition to be ignored.
- Alarm configuration can limit the severity of an active alarm.
- Alarm configuration specifies the severity with which an active digital alarm is reported.
- Alarm configuration specifies the Hold Time for an active alarm.
- Alarm configuration specifies the thresholds and hysteresis used to detect alarm conditions for analogue alarms.

The third factor that affects the alarm state is alarm acknowledgement. Once the device operator has received knowledge of the occurrence of an active alarm, he can indicate this to the ENX device by acknowledging the alarm. The ENX device will then ignore this alarm in the calculation of the global device alarm state so that newly occurring alarms will immediately be brought to the operators attention.

Given all the influences explained above, the alarm can be in one of the following states:

Not Available

This indicates that the alarm condition is not available. The alarm is always considered considered to be inactive in this case and the corresponding alarm state value is "n.a.".

Inactive

This indicates that the alarm condition is inactive. The alarm is always considered to be inactive in this case and the corresponding alarm state value is "Ok".

Ignored

This indicates that the alarm condition is active, but the alarm condition was configured to be ignored. The alarm is always considered to be inactive in this case and the corresponding alarm state value is “Ignored”.

Acknowledged

This indicates that the alarm condition is active and the alarm is not configured to be ignored. However, the device operator has acknowledged the alarm and the corresponding alarm state value is “Acknowledged”.

Warning

This indicates that the alarm condition is active and the alarm is considered to be active, having a severity of “Warning”.

This state occurs for analogue alarms if a warning threshold has been crossed, but the corresponding error threshold is not yet reached. This state occurs for digital alarms if the alarm was configured to be a “Warning” by the device administrator.

A warning level usually indicates that the device is operating close to the limits of the operational parameters and that actions should be taken to ease the situation.

Error

This indicates that the alarm condition is active and the alarm is considered to be active, having a severity of “Error”.

This state occurs for analogue alarms if an error threshold has been crossed. It occurs for digital alarms if the alarm was configured to be an “Error” by the device administrator.

An error level usually indicates that the device is operation outside of the limits of the operational parameters and that the device is no longer operating reliably.

Alarm Acknowledgement Behaviour

Any active alarm can be acknowledged by the device operator. Even though the alarm condition is still active, this has the effect of making the alarm “silent” by excluding it from the global device alarm state calculation. Informally speaking, this makes the alarm a “known problem”.

It may happen that the alarm severity changes while the alarm is acknowledged. In case of analogue alarms this may happen if an additional threshold is crossed, whereas for digital alarms it implies a configuration change. In any case, the severity of the acknowledged alarm may either increase (from “Warning” to “Error”) or decrease (from “Error” to “Warning”). Any other value (“Ignored”, “Inactive” or “Not Available”) means that the alarm becomes inactive.

The device administrator can select from three different policies that decide whether the alarm gets reactivated by the alarm severity change or remains acknowledged. This is a global setting and valid for all alarms.

Keep Acknowledged Until Inactive

This policy keeps acknowledged alarms in their acknowledged state until the alarm becomes inactive. Neither the increase nor the decrease of the alarm severity have any effect.

Unacknowledge When Raising Severity

This policy keeps the alarm acknowledged as long as “the situation gets better”. When the severity decreases from “Error” to “Warning”, the alarm remains acknowledged. However, if the situation gets worse and the alarm severity increases from “Warning” to “Error”, the alarm is reactivated and brought again to the device operators attention. This is the default behaviour.

Unacknowledge on State Change

This policy will always reactivate an acknowledged alarm whenever the alarm severity changes.

Example

The next figure displays an example, of temperature alarm and the behaviour when alarm is raised, acknowledged and raised again.

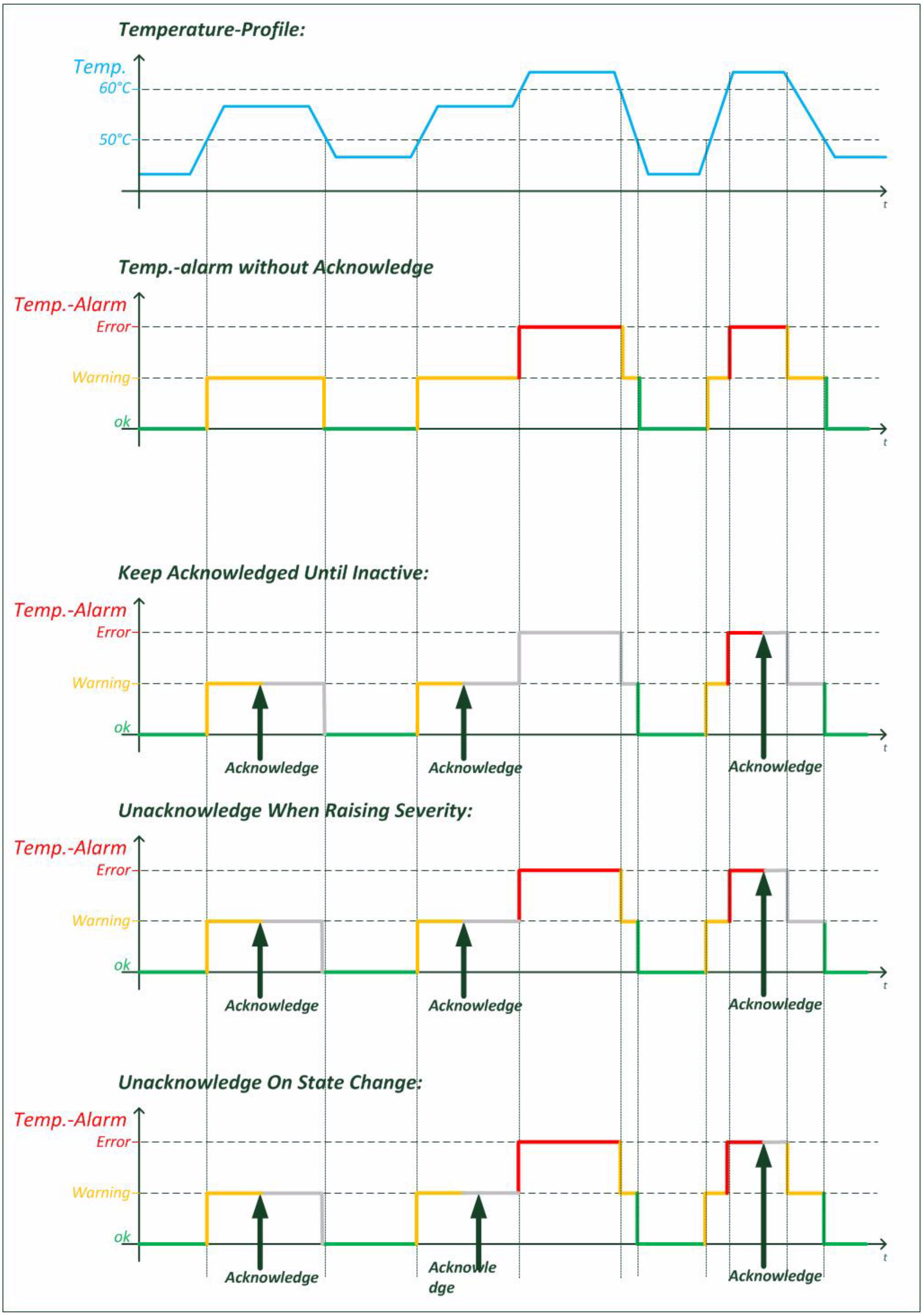


Figure 4-4 *Acknowledge of Alarms*

Alarm Properties

Each alarm has a certain set of properties associated with it that depends on the alarm type (analogue or digital alarm).

Common Alarm Properties

These properties are defined for both, analogue and digital alarms.

- Alarm Group: the group that the alarm belongs to (see below).
- Alarm Name: a descriptive name of the alarm.
- Alarm Value: the current value of the observed quantity.
- Alarm State: the current alarm state.
- SNMP Notification: whether to generate SNMP traps if the alarm state changes (editable).
- Hold Time: The hold time indicates the minimum time an alarm is active after rising. This is to reduce the number of alarms in a certain time-frame and to tune the system to special requirements.

Digital Alarm Properties

Digital alarms have one further property:

- Alarm Severity: the device administrator must decide for each digital alarm whether it represents an error condition, a warning condition, or an ignorable condition (editable).

Analogue Alarm Properties

Besides the common alarm properties, analogue alarms have the following properties as well:

- Overrun Warning Threshold: If the physical quantity has a meaningful upper limit for its operational range, the threshold above which the alarm becomes active with “Warning” severity (editable).
- Overrun Error Threshold: If the physical quantity has a meaningful upper limit for its operational range, the threshold above which the alarm becomes active with “Error” severity (editable).
- Underrun Warning Threshold: If the physical quantity has a meaningful lower limit for its operational range, the threshold below which the alarm becomes active with “Warning” severity (editable).
- Underrun Error Threshold: If the physical quantity has a meaningful lower limit for its operational range, the threshold below which the alarm becomes active with “Error” severity (editable).
- Hysteresis: A hysteresis applied to threshold values when checking whether an active alarm condition is cleared (editable).

Alarm Groups

Due to the large number of alarms already defined, the alarms are divided into a number of different alarm groups. These alarm groups serve multiple purposes:

- Logical subdivision of alarms for a better overview.
  - Alarms are grouped by function or hardware component they refer to (e.g. “System Alarms” for general device management alarms, “Clock Alarms” for SyncE and PTP-related alarms, …)
- Alarm status summary.
  - The alarm group keeps track of the most severe alarm state of any alarm in the group and provides the current number of alarms that are ignored, acknowledged, or are active with “Warning” or “Error” severity.
- Easy acknowledgement of multiple alarms.
  - All alarms within an alarm groups can be acknowledged with a single action.
- Limiting the alarm severity of multiple alarms.
  - The alarm group defines a maximum alarm severity setting that overrides the alarm severity of all alarms in the alarm group.

Global Alarm Status

The SCX2e device provides a summary of all alarms. Besides showing the number of acknowledged alarm and active alarms with “Warning” or “Error” severity, the global (overall) alarm status keeps track of the maximum severity of any active alarm. Furthermore, the global alarm status is reflected by the ALM-LED on the front panel of the device and the alarm relay.

The ALM-LED will be turned on if the global alarm state is “Error”, it will blink if the global alarm state is “Warning” and be turned off otherwise.

The alarm relay will be activated if the global alarm state is “Error” and be deactivated otherwise.

Active Alarm List

The Active Alarm List is an overview to all alarms which are active at the current moment. When an alarm turns to “Warning” or “Error” it will be added to this list. When the alarm returns inactive state, it will be removed from this list without further notice. Any “ignored” alarm is also not shown in the Active Alarm List.

When an alarm is acknowledged, it will remain in the “Active Alarm List”, but it will be re-sorted at a lower level.

For the time being, the Active Alarm List is ordered by

1. Alarm Severity (Error - Warning - Acknowledged),
2. Group Name (alphanumeric order) and
3. Alarm Name (alphanumeric order).

Date & Time Settings

The SCX2e does have an internal clock, which can be set by either user or via NTP-server(s). This gives the SCX2e the chance to provide proper time-stamps in logging and alarms. In case of power-failure, the SCX2e will keep the correct date and time for a period of at least 10 days.

NOTE: After 10 days without power supply, the internal clock of the SCX2e has to be re-set again.

If there is no NTP-server is configured in the designated variables, the NTP feature is disabled. In this case, the date, time and time-zone can be specified by user during installation process or whenever needed.

The SCX2e does support versions and version 4 of NTP:

- NTPv3 ([IETF RFC 1305]).
- NTPv4 ([IETF RFC 5905]).

Up to 8 different servers may be configured on the SCX2e to make sure always a valid link to an available time-server is found.

When the device can’t get (valid) timing information of the given NTP-servers, an alarm can be raised to indicate this problem. The NTP-Status alarm can be found in the System alarm group.

NTP and Encryption

NTP provides an accurate hardware time reference for network infrastructure. It can pose a security risk, particularly if malicious users attempt modifying or replicate time-stamps in order to generate a false time on a networked computer or device.

Therefore the SCX2e works with authentication on NTP to overcome the inherent security risks and ensuring that any response received from a time server was generated from the intended reference. Basically, the SCX2e sends a request for time to a NTP-server. The server responds to the SCX2e with a time-stamp along with any one of a number of pre-agreed encrypted keys. On receipt of the time-stamp, the SCX2e un-encrypts the supplied key and verifies it against a list of trusted keys. The SCX2e can then be sure that the received time-stamp was indeed transmitted from the intended server. SCX2e utilizes MD5 encryption (Message Digest Encryption 5), which is a 128-bit cryptographic hash function, which outputs a fingerprint of the key.

Configuration Management

The (actual) configuration of the SCX2e can be stored locally and remote (via SFTP) to recall it later or to use it as profile for other devices. The configuration is stored in a special file-format (*.cfgx) which is protected against not allowed changes and keeps the data-base clean and consistent. Any change of settings, which are not made in the correct context could lead into inconsistency and this is avoided here.

It can be necessary that some items of the current configuration shall not be stored, as these settings shall not be used in the future. Or a stored configuration shall not be taken in total, but only partial. A reason could be that the stored IP-address is not longer valid and the actual address shall not be overwritten by the new configuration. For this reason some topics can be selected to be stored or not stored and/or overwritten or kept during (re-) call of configuration:

Item	Description
IP Config MGMT1	All the IP settings for MGMT1 interface (out-of-band management port), including: IP-address, net-mask, Default-GW and VLAN-tag (if defined).
IP Config MGMT2	All the IP settings for MGMT2a interface (out-of-band management port), including: IP-address, net-mask, Default-GW and VLAN-tag (if defined).
SNMP Trap Targets	All SNMP trap-receiver, including: IP-address, UDP-port, user-name, SNMP-version and state.
SNMPv2 Communities	All defined communities, including: Name, access-level and state.
SNMPv3 User	All defined users, including: Name, authentication, access-level, encryption and state.
SSH keys	All defined SSH-keys, including: Cipher, key-ID, user, comment and state.
User Accounts	All local stored user-accounts, including: Password, user-group and state.
All Other Configuration	All the rest of configuration. Of course this can be not stored or denied during re-call to have e.g. pure account profiles.

Diagnostics

Wrong IP settings or un-proper setup of cables are often causes for problems in the network. To check all these, the diagnostic-menu is implemented to the SCX2e. The reachability of a given IP-address of remote host or router can be tested by

- PING command,
- Trace route (via UDP),
- Trace route (via ICMP).

The result is presented as command output and helps to get better view of your (management) network.

Logging

The SCX2e does provide a logging function, which notices all events in the log-file. This file is stored onboard and the last 999 entries can be (re-)viewed. If necessary the log-file can be stored on a server or downloaded via http.

The events, which are added to the log-file, are divided into 4 groups:

- Information: Messages from the SW about system status and successful started or stopped applications. An information entry is indicated by the <INFO> label.
- Alarm: All variables, which can raise an alarm, will be logged, when the alarm gets error-, warning- or idle-state. An alarm entry is indicated by the <ALARM> label, followed by <ERR>, <WARN> or <OFF>.
  An alarm-variable, which is configured as “ignore” will not be added to the log-file, independent from its status. It is ignored.
- Audit: The audit entry is added to the log-file, when the configuration of the device is changed by user. This action is logged for better traceability. The audit entry is indicated by the <AUDIT>-label.
- Device-Error: This are failed attempts to login to the device or the device detects an extraordinary status.Device-errors may be solved by the SW itself by restarting applications, but it can be an indicator for severe problems.

Each entry in the log-file has the date/time information, when the event did occur, followed by the type-label and a short description about the event. Some examples are listed below:

<INFO>

```
2013-01-22 09:15:54  < INFO> Rebooting device
2013-01-22 13:01:17  < INFO> Starting HTTP server
2013-01-22 13:01:20  < INFO> System started.
2013-01-22 13:01:20  < INFO> Starting SNMP server
2013-01-22 14:03:25  < INFO> Web login via LOCAL authentication from 192.168.1.1: admin
(admin)
2013-01-22 14:47:08  < INFO> CLI login via LOCAL authentication from CONS: admin
(admin)
```

- The <INFO>-entry gives information about started applications and attempts to login.

<AUDIT>

```
2013-01-22 09:15:54  <AUDIT> Administration/Reset System/Start Reset executed by admin
from CONS (cli)

2013-01-22 14:07:07  <AUDIT> Alarm Management/LAN 1 <...> Alarms/Group Details/Link
Status/Settings/Alarm Severity set to “Warning” by admin from 192.168.1.1 (web)

2013-01-22 14:07:25  <AUDIT> Alarm Management/LAN 2 <...> Alarms/Group Details/Link
Status/Settings/Alarm Severity set to “Ignore” by admin from 192.168.1.1 (web)
```

- The <AUDIT>-entry traces the changes of configuration.

<ALARM>

```
2013-01-22 13:01:05  <ALARM> [ERR] : SFP removed
2013-01-22 14:07:54  <ALARM> [OFF] LAN 1: Link Up
2013-01-22 14:08:16  <ALARM> [WARN] LAN 1: Link Down
2013-01-22 14:08:22  <ALARM> [OFF] LAN 3: Link Up
2013-01-22 14:08:31  <ALARM> [ERR] LAN 3: Link Down
```

- The <ALARM>-entry traces the alarm status of the system.

<ERROR>

```
2013-01-22 14:47:02  <ERROR> CLI authentication failure from CONS: admin
```

- The <ERROR>-entry indicates an unsuccessful try to login.

Chapter 5
SCX2e Web-GUI

The SCX2e can be configured via a html-based Web-GUI (Operator Interface). Just a standard web-browser is needed and an IP-connection to the device. This chapter will explain how to connect to the Web-GUI and its usage.

NOTE: A detailed presentation of all Web-GUI variables and menus is given in [axRefGuideWebGUI_SCX2e].

Introduction

Access to the Device

The SCX2e Web-GUI can be accessed via the both management ports (called “MGMT1” and “MGMT2” interface). Both interfaces use different IP-addresses, but the behaviour and the usage from html-point of view is just the same.

arcutronix’ devices are proved to be used with different web-browsers:

• Internet Explorer (Microsoft):	IE 7 or higher
• Mozilla Firefox (Open Source):	Firefox 6 or higher
• Opera (Opera Software ASA):	Opera 10 or higher
• Safari (Apple):	Safari 5 or higher
• Google Chrome (Google):	Chrome 9.0 or higher

Security Issues

The Web-GUI is accessible via any TCP/IP link to the device, so it might be that other persons than the intended ones get connection and will see the login screen. To avoid forbidden configuration or burglary of information, the access is protected against intruders via user-name and password. Any not successful attempt to login to the device is stored in the log-file and a trap can be configured to inform higher level management system about this.

Any time you connect or reconnect to the initialized SCX2e the login-window is displayed and a password request turns up on the terminal.

Be careful with passwords! If you write them down, keep them in a safe place. Do not choose strings easy to hack. In particular, do not use the default strings which were valid when you received the device.

Do not forget your password. If you forget your password the device will be rendered useless and will have to be sent back to the factory for basic re-configuration.

NOTE: Three different access-level are selectable with different access rights:

1. Guest (only view)
2. User (view and modify)
3. Admin (full access inclusive user administration)

When the device is started-up the very first time, only the user “admin” is defined. See in “User & Access Administration” on page 4-2, how to define the other users and how to change the user password.

Web-Menu Body

Login Screen

After a management connection has been established towards the SCX2e, the login screen is displayed. The management software may be accessed by the user with different access levels (see “Security Issues” on page 5-1).

The Login screen is shown in the figure below. For a first quick overview, the type, name, alarm status and the serial number of the connected device is displayed on the top-right side. This makes it easy to verify, whether one has reached the right unit (the entered URL might be wrong or mistyped) and its actual status. If all is fine, it might be no need to login and one can turn towards the next device to check and work with.

The fields user-name and passwords must be filled and after pressing the “Login”-button, the inscription is verified against the local or remote data-base. If the login is accepted, the next screen will open, otherwise the login attempt is denied and one will remain on this screen.

NOTE: A refused attempt to login to the unit is logged.

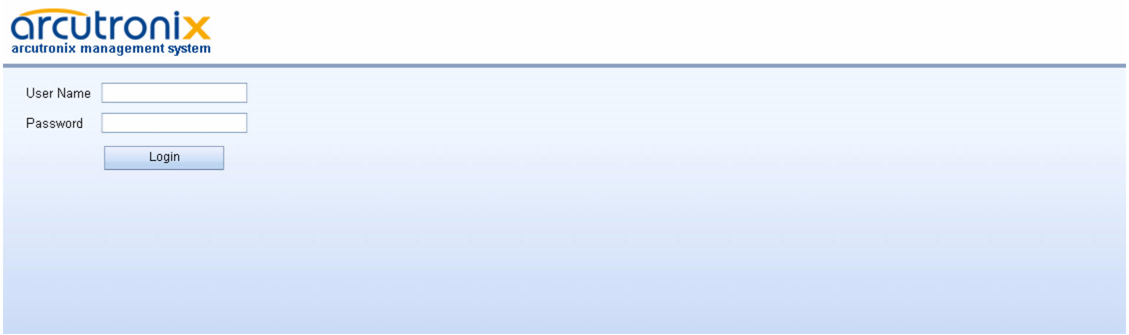


Figure 5-1 *Login Screen*

A user name and a valid password have to be entered before access to configuration parameters is granted. The default user name and password are as follows:

User:	admin
Password:	private

CAUTION: It is strongly advised to change these passwords in the USER ADMINISTRATION menu after the first login.

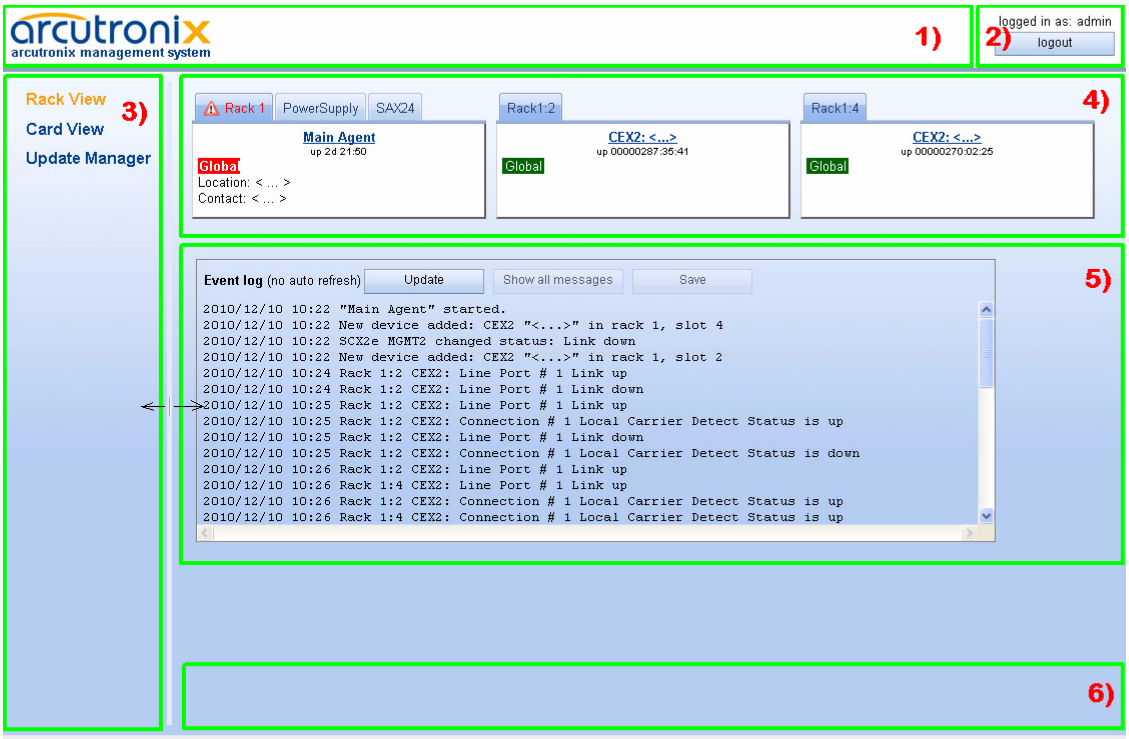
If the device is started-up the very first time, the only user 'admin' is defined with the password 'private', which should be changed immediately after login. The password is not displayed, each character is replaced by an asterisk (*). An error message will be displayed for any unsuccessful login (the application continues with the login menu).

NOTE: Be careful, when typing user and password. The Web-GUI is case-sensitive.

Layout of Web-GUI

After Login, the SCX2e Web-GUI is seen in its full glance. The Web-GUI is designed according the latest rules for web-based GUIs and you will find it very easy to navigate.

The Web-GUI's body is divided in 5 major parts, which are shown in the next figure and will be explained a little bit after this.



```
2010/12/10 10:22 "Main Agent" started.
2010/12/10 10:22 New device added: CEX2 "<...>" in rack 1, slot 4
2010/12/10 10:22 SCX2e MGMT2 changed status: Link down
2010/12/10 10:22 New device added: CEX2 "<...>" in rack 1, slot 2
2010/12/10 10:24 Rack 1:2 CEX2: Line Port # 1 Link up
2010/12/10 10:24 Rack 1:2 CEX2: Line Port # 1 Link down
2010/12/10 10:25 Rack 1:2 CEX2: Line Port # 1 Link up
2010/12/10 10:25 Rack 1:2 CEX2: Connection # 1 Local Carrier Detect Status is up
2010/12/10 10:25 Rack 1:2 CEX2: Line Port # 1 Link down
2010/12/10 10:25 Rack 1:2 CEX2: Connection # 1 Local Carrier Detect Status is down
2010/12/10 10:26 Rack 1:2 CEX2: Line Port # 1 Link up
2010/12/10 10:26 Rack 1:4 CEX2: Line Port # 1 Link up
2010/12/10 10:26 Rack 1:2 CEX2: Connection # 1 Local Carrier Detect Status is up
2010/12/10 10:26 Rack 1:4 CEX2: Connection # 1 Local Carrier Detect Status is up
```

***Figure 5-2** Web-GUI's Appearance*

1. Logo/Family Pane.
2. Info Pane: Info about
   - device-type (here SCX2e),
   - device-name (here Demo-Device),
   - serial number,
   - and alarm status (status icon).
3. Login/Logout Pane: Info, who is logged in and a button for Logout.
4. Navigation Pane: Navigating in the Web-GUI is easy with the Navigation Pane. The settings are grouped in different categories, which can be exploded and collapsed.
5. Main Pane: This is the pane, where all the information is listed and the configuration can be changed and adopted. The next chapter will mainly handle the settings in this section.
6. Alarm-Table: Summary of all events and alarms.
7. Message Pane: Here status and error-messages are shown.

Navigation

The Web-GUI is a graphic user menu. The best way to navigate between the different pages is to use your mouse. Open and collapse the menus in the Explorer-Bar (see above) and select the page, you want to see and/or edit.

Select a menu entry

When you move the mouse-pointer over the explorer-bar, you can see the pointer change its face: When you move the pointer over a selectable item, it will look like a this: ☝, if there is no selectable value, it is standard (normally arrow): ↖

When you want to open or select the given entry, press the left button on your mouse to complete the selection.

The selected menu-entry is displayed in orange-coloured text, while all the others are marked blue (see Figure 5-2).

In some cases, you will find lists to select an entry. Use also the mouse-pointer to navigate in these list. Press Enter, when the right entry is highlighted to select it.

Page Update

To update the actual menu, just use your browser's reload button.

Logout

Use the Logout-Button to terminate the session and leave the unit. Never forget to logout, as otherwise unauthorized persons could get access to the unit and damage your services.

The auto-logout feature adds additional security in case the regular logout has been forgotten.

WARNING: If your PC/Laptop is very busy and does not reply on the devices cyclic “Hello”-messages, the web-session will be terminated after 90 seconds without reply. This auto-termination is implemented due to security reasons if you close your browser or browser-tab without logout.

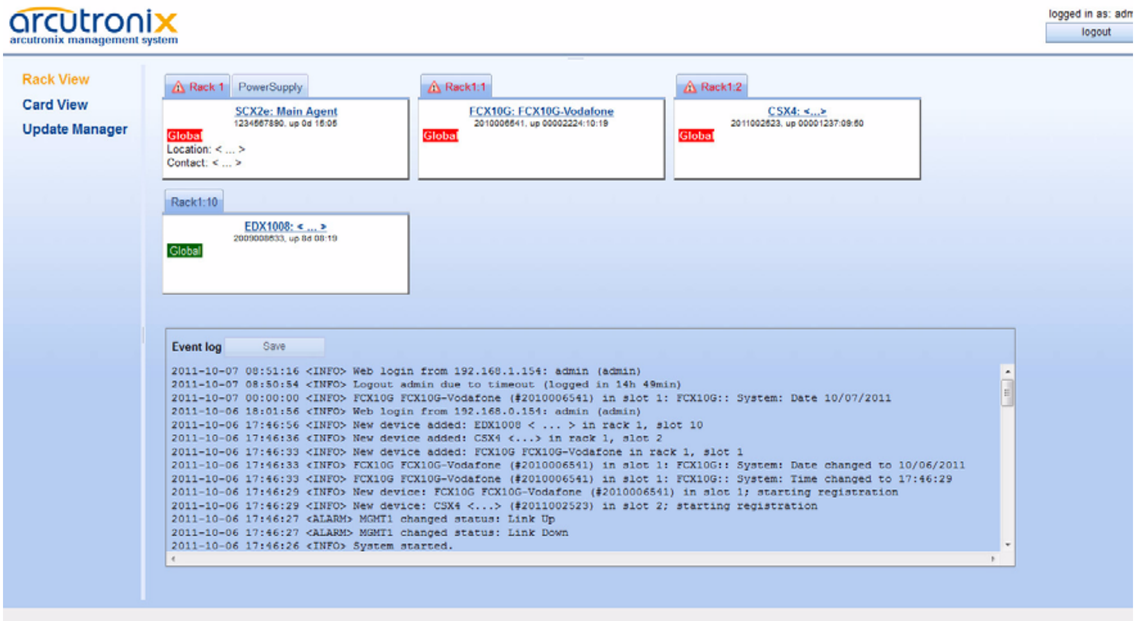
Rack View

The “Rack View” is the presentation of the information and actual status of all cards in a general overview of the ax MSP rack. All discovered cards are shown in parallel and a summery for each is given. The summery shows short information like serial number, user’s given name, slot-ID, up-time, and alarm-status.

If remote cards are detected, which can be detected and managed by the local agent, the remote cards and local card are grouped into one icon with (at least) two tabs. Each tab represents one of the discovered (line-) cards. Using this presentation, it is easy to see, which cards are physically connected.

Move the mouse over one of the shown cards and you can enter the Card-View of the device.

On the bottom area of the “Rack-View” the logging windows is presented. The logging window shows all entries to the log-file. Details about the logging-window and the messages are given in “Logging” on page 4-24.



```
2011-10-07 08:51:16 <INFO> Web login from 192.168.1.154: admin (admin)
2011-10-07 08:50:54 <INFO> Logout admin due to timeout (logged in 14h 49min)
2011-10-07 00:00:00 <INFO> FCX10G FCX10G-Vodafone (#2010006541) in slot 1: FCX10G:: System: Date 10/07/2011
2011-10-06 18:01:56 <INFO> Web login from 192.168.0.154: admin (admin)
2011-10-06 17:46:56 <INFO> New device added: EDX1008 < ... > in rack 1, slot 10
2011-10-06 17:46:36 <INFO> New device added: CSX4 <...> in rack 1, slot 2
2011-10-06 17:46:33 <INFO> New device added: FCX10G FCX10G-Vodafone in rack 1, slot 1
2011-10-06 17:46:33 <INFO> FCX10G FCX10G-Vodafone (#2010006541) in slot 1: FCX10G:: System: Date changed to 10/06/2011
2011-10-06 17:46:33 <INFO> FCX10G FCX10G-Vodafone (#2010006541) in slot 1: FCX10G:: System: Time changed to 17:46:29
2011-10-06 17:46:29 <INFO> New device: FCX10G FCX10G-Vodafone (#2010006541) in slot 1; starting registration
2011-10-06 17:46:29 <INFO> New device: CSX4 <...> (#2011002523) in slot 2; starting registration
2011-10-06 17:46:27 <ALARM> MGMT1 changed status: Link Up
2011-10-06 17:46:27 <ALARM> MGMT1 changed status: Link Down
2011-10-06 17:46:26 <INFO> System started.
```

Figure 5-3 *Rack-View*

Symbols of the Rack View

Each plugged module (line-card etc.) in the sub-rack does have an rectangular diagram in the rack-view. On top of the diagram one or more flags are seen to indicate that this diagram contains more information. The flag shows the status of the card in a small icon. If there is no icon to see, all is fine and the card is working without any problems.

Table 5-1 *Status-Symbols*

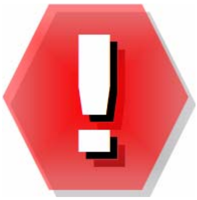
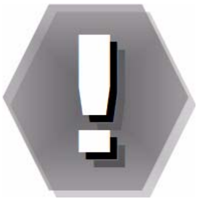
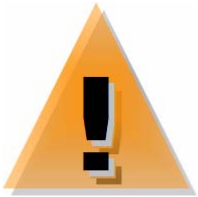
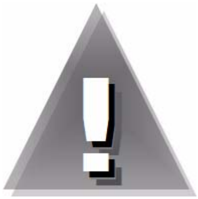
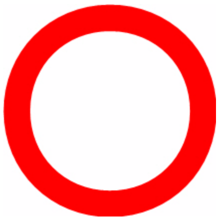
Symbol	Prio	Meaning
none (empty)	0	Everything is fine. No problems detected.
	4	Alarm-Symbol. The device has detected at least one active alarm.
	2	Alarm-Acknowledged Symbol. The device has at least one alarm, which is already acknowledged by user.

Table 5-1 Status-Symbols (continued)

Symbol	Prio	Meaning
	3	Warning-Symbol. The device has detected at least one active warning.
	1	Warning-Acknowledged Symbol. The device has at least one alarm, which is already acknowledged by user.
	5	Removed-Symbol. The device was removed or fails. If the device shall be removed permanently, please delete the diagram from rack-view.

As there can be only one symbol at the time, there is a priority. Depending on the priority of the event, the symbol with the highest priority is shown. This starts with the “Removed” and ends up with none-symbol, which indicates All-Good.

Card View

The “Card View” is the presentation of the information and actual status of all cards in a detailed form. All discovered cards can be selected and detailed configurations can be done then. While the “Rack View” is the overview section of the menu, the “Card-View” is the operating and configuration section. Only when cards a selected in the “Card View” changes in configuration can be done.

Each type of card, does have its individual card-view appearance. Though many items will be very similar on all devices, one can not present a common valid overview. New types of line-cards may have different appearances. Even new features on existing line-cards may have the result, that the appearance is different. as this document is intended to be stable, even when new line-cards, features and services are available, not all card-views of all cards can be presented here. Hereafter, only the card-view and management options for the agent itself will be presented.

Web-Menus of SCX2e

To enter the card view of the SCX2e select it in the Rack-View or in the Navigation Pane. The card’s individual menu appears. After selecting the SCX2e the main view is displayed, which provides a general overview of the menu structure.

All menu entries and the optional usage and settings are explained in detail in an extra document: [axRefGuideWebGUI_SCX2e]. Please refer to this document for details.

Chapter 6
SNMP and MIBs

This chapter provides information on the SNMP and the management information bases (MIBs) used by the SCX2e.

SNMP Access Generally

The growing global network ‘Internet’ was the home of plans to simplify network maintenance by defining a maintenance protocol, which would allow network managers to control network equipment via the network itself. This protocol was given the name SNMP (Simple Network Management Protocol). As the name implies, SNMP was originally planned as an intern solution. However, SNMP became widely used and is now a universal standard.

What is the difference between equipment with and without SNMP? Generally, SNMP featured equipment has:

- Added intelligence to talk SNMP and to get and set unit parameters
- An own unique network address
- Some kind of local management port

Network management by SNMP requires at least two partners:

- Network equipment with SNMP software, called ‘agent’
- A network station, running some kind of network management software

The two partners communicate via the net using SNMP. The network management station sends configuration commands and data requests to the network equipment. The network equipment responds to requests by sending the requested data. Additionally, traps are triggered by certain events in the network equipment. Traps are data packets containing information about these events. Their destination is a (or multiple) network management station, where the information is collected. SNMP traps enable an agent to notify the management station(s) of significant events by way of an unsolicited SNMP message.

Network configuration information, in particular configuration commands, is sensitive data and must therefore be protected against prying eyes. SNMP deals with this problem by implementing something called a ‘community’. A community is comparable to a password and gets attached to each SNMP message. The attached community allows the receiving SNMP partner to decide if the transmitting partner is allowed to force the execution of the command.

The arcutronix Multi Service System supports two versions of SNMP: SNMPv2c (version2, community-based) and SNMPv3.

SNMPv2c

Community-Based Simple Network Management Protocol version 2, or SNMPv2c, is defined in [IETF RFC 1901]. SNMPv2c revises version 1 and includes improvements in the areas of performance, confidentiality, and manager-to-manager communications. It introduced GETBULK, an alternative to iterative GETNEXTs for retrieving large amounts of management data in a single request. SNMPv2c uses the same simple community-based security scheme as the former variant SNMPv1. While officially only a "Draft Standard", this is widely considered the de facto SNMPv2 standard.

SNMPv3

SNMPv3 makes no changes to the protocol aside from some addition of cryptographic security. SNMPv3 primarily added security and remote configuration enhancements to SNMP. Security has been the biggest weakness of SNMP since the beginning. Authentication in SNMP Versions 1 and 2 amounts to nothing more than a password (community string) sent in clear text between a manager and agent.

Each SNMPv3 message contains security parameters which are encoded as an octet string. The meaning of these security parameters depends on the security model being used.

SNMPv3 provides important security features:

- Confidentiality - Encryption of packets to prevent snooping by an unauthorized source.
- Integrity - Message integrity to ensure that a packet has not been tampered with in transit including an optional packet replay protection mechanism.
- Authentication - to verify that the message is from a valid source.

Traps

SNMP encourage trap-directed notification. The idea behind trap-directed notification is as follows: if a manager is responsible for a large number of devices, and each device has a large number of objects, it is impractical for him to poll or request information from every object on every device. The solution is for each agent on the managed device to notify the manager without solicitation. It does this by sending a message known as a trap of the event or NOTIFICATION.

After receiving the event, the manager displays it and may choose to take an action. For instance, the manager can poll the agent directly, or poll other associated device agents to get a better understanding of the event.

Trap-directed notification can result in substantial savings of network and agent resources by eliminating the need for frivolous SNMP requests. However, it is not possible to totally eliminate SNMP polling. SNMP requests are required for discovery and topology changes. In addition, a managed device agent can not send a trap, if the device has had a catastrophic outage.

Installation Prerequisites

This section provides the installation prerequisites for SNMP.

Prerequisites for SNMP management:

- A management station with an Ethernet 10/100BaseT respectively RS232 interface.
- Management software for SNMP management (e.g. SNMPc, HP Openview).
- A VT100 compatible terminal or PC with terminal software (only used for initial installation).

Preparing the SNMP Management System

Before managing the SCX2e by SNMP, one has to prepare the SNMP management system. First install the MIBs for the SCX2e and second configure the correct access parameters.

You can download the MIB from the ax intranet (www.arcutronix.com/customer):

Login:	**User = p49170644-0** **Password = 1qayxsw2**

A MIB (Management Information Base) is a kind of database, which tells the network management station about specific capabilities of the new equipment. Add the contained MIBs to the MIBs already known to your management system. Generally, you have to recompile the MIB database to include the new information.

Configure your management station to use SNMPv2c for read and write access mode and enter the community strings for read/write and read-only access.

Management Information Bases (MIBS)

The MIBs (Management Information Bases) define the variables which are used to control a (SNMP-) device or to retrieve operational data from the device. The MIB consists of collections of managed objects identified by object identifiers (see below). MIBs are accessed using the simple network management protocol (SNMP). A managed object (sometimes called a MIB object or an object) is one of a number of characteristics of a managed device.

System MIB variables are accessible through SNMP as follows:

- Accessing a MIB variable—Function is initiated by the SNMP agent in response to a request from the NMS. The agent retrieves the value of the requested MIB variable and responds to the NMS with that value.
- Setting a MIB variable—Function is initiated by the SNMP agent in response to a message from the NMS. The SNMP agent changes the value of the MIB variable to the value requested by the NMS.

An object identifier (OID) uniquely identifies a MIB object on a managed network device. The OID identifies the MIB object's location in the MIB hierarchy, that can be depicted as a tree with a nameless root. The levels of which are assigned by different organizations, such as IANA. This model permits management across all layers of the OSI reference model.

The MIBs for arcutronix's SNMP management are based on the arcutronix naming convention. The root-OID tree structure is accessible via

iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).**arcutronix(30507)**

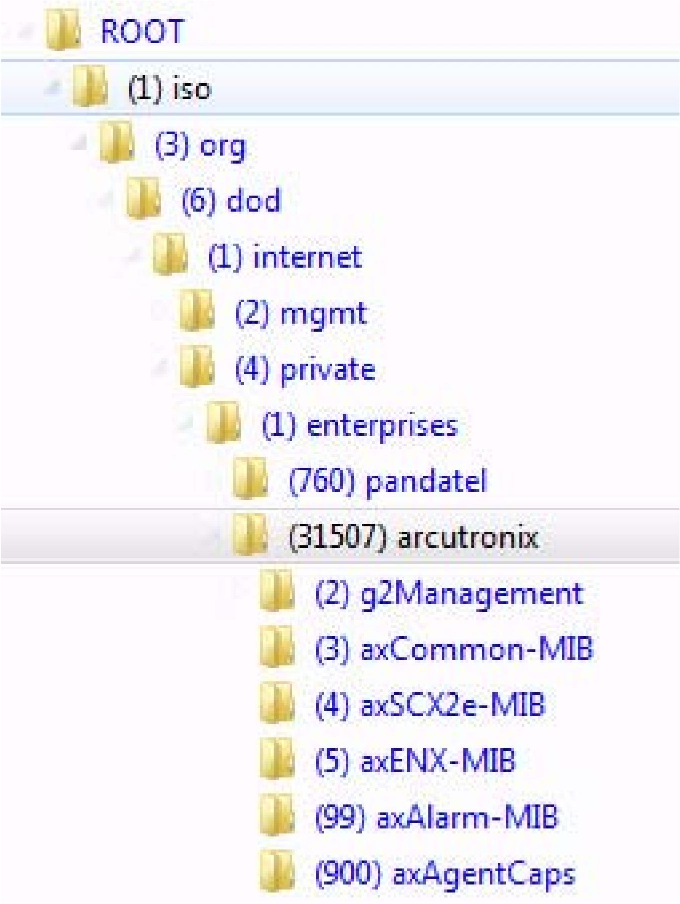


Figure 6-1 *The SNMP ax-MIB Tree (1.3.6.1.2.4.1.31507)*

Each number in the OID corresponds to a level of MIB hierarchy. For example, the OID 1.3.6.1.4.1.31507.3.xyz represents the .xyz with the location in the MIB hierarchy as follows. (Note that the numbers in parentheses are included to help show correspondence to the MIB hierarchy. In actual use, OIDs are represented as numerical values only.)

iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).arcutronix(31507).axCommon-MIB(3).nn-MIB

The format of the MIBs as well as global sections are defined in the SNMP standard. MIBs are written in a special language (ASN 1) and are plain ASCII text. Thus they can be read using any available editor.

The MIBs can be enhanced at any time, so please refer to the MIBs itself for documentation.

Chapter 7
SSH and CLI

The SCX2e can be configured via a text-based Command Line Interface (CLI), which can be reached over a Secure Shell (SSH) connection. For the SSH-connection, only a SSH-client and an IP-connection to the device is needed.

This chapter will explain how to connect to the CLI/SSH and the usage of CLI.

NOTE: A detailed presentation of all CLI variables and menus is given in [axRefGuideCLI_SCX2e].

Access to the Device

The SCX2e CLI can be accessed via the management ports. The ports have different IP-addresses, and might be grouped to combo-ports. But the behaviour and the usage from SSH/CLI point of view all ports are operated in the same way.

The setup for the SSH connection will be explained in the following chapter.

SSH Connection

To establish the SSH connection between SCX2e and client a user-name/password or a key is required. Several options can be selected by the administrator.

The SSH protocol is using a TCP/IP connection. As default, TCP port 22 is used for it. If necessary, this can be changed.

Using User-Name and Password

The SSH connection is established by using one of the user-names and password, which are defined locally or by NAS. See chapter “User Administration” on page 4-36 for defining local users and usage of TACACS+.

As soon as user-name and password are verified and the access is granted, the SSH-connection is established and the login to the CLI is done. No further inquiry is needed.

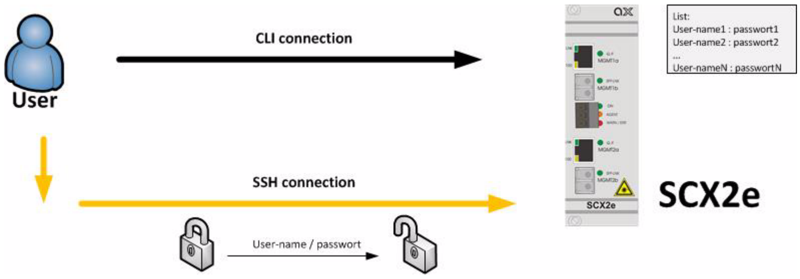


Figure 7-1 *SSH-connection using User-Name and Password*

Using Global SSH-Password

The SSH connection is established by using a dedicated user-names (“cli”) and a special password, which is defined locally. The user “cli” is pre-defined on the device, the “Global SSH-Password” must be configured. This option is intended to define a common (“global”) SSH-access for all devices to make SSH-connection independent from user’s login data.

The user “cli” and the global SSH-password is solely used to establish the SSH-connection. After successful SSH-setup, the user is asked for his login data (user-name and password). The user’s login data may be locally stored and/or on a NAS. See chapter “User Administration” on page 4-36 for defining local users and usage of TACACS+.

NOTE: The global SSH-password must fulfil minimum demands on security. It is required to use lower- and upper-case letters and digits. The minimum length of the password is 8 characters. If the internal check for strength of password fails, an error message will be sent.

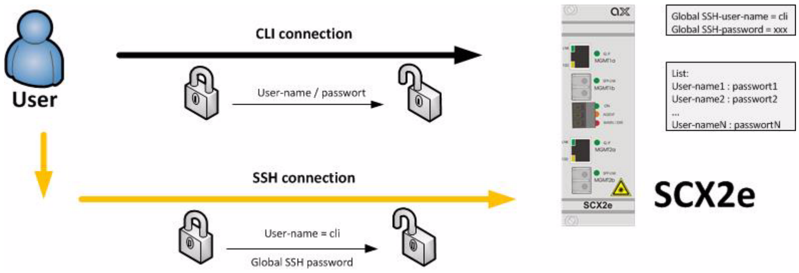


Figure 7-2 *SSH-connection using Global SSH-Password*

Using SSH-Key

A more secure method of authentication is through the use of RSA keys. The basic principle is as follows: RSA involves a public key and a private key. The public key can be known to everyone and is used for encrypting messages. Messages encrypted with the public key can only be decrypted using the private key.

Any host to which the user wants to connect must be aware of his public RSA key, as the server uses it during the authentication process. The user must place his public key living on the originating client machine, into his own authorized_keys file on the server.

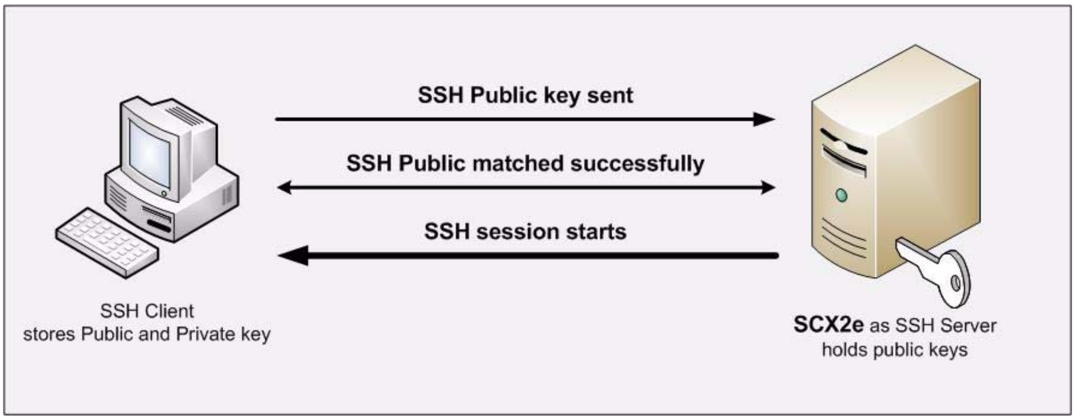


Figure 7-3 *Secure Shell - Public Key*

When the user wants to connect to that server, SSH will first negotiate an encrypted session, then send the server the client's public key. The server checks that the public key is in the user's authorized_keys. If so, the server sends the client a challenge (a random number encrypted with the user's public key). If the client can then send back the random number decrypted, it has just proven that it has the private key (there is no other way to decrypt the challenge number), and is therefore authentic.

The user's private key is a very sensitive piece of data - with it, anyone can connect to any host on which the corresponding public key is in the authorized_keys. Therefore, the user's private key is never written to disk decrypted.

Public key authentication solves this problem. You generate a key pair, consisting of a public key (which everybody is allowed to know) and a private key (which you keep secret and do not give to anybody). The private key is able to generate signatures. A signature created using your private key cannot be forged by anybody who does not have that key; but anybody who has your public key can verify that a particular signature is genuine.

The Authentication layer uses one or more of the following authentication methods to validate the user:

1. Password Authentication
2. RSA/DSA Public-Key Authentication
3. Kerberos Authentication
4. Host-based Client Authentication

We have focused only on the RSA Public-Key based Authentication in this process.

NOTE: The SSH-key, which is stored on the device is a public key. The SCX2e expects that the file name's extension is "*.pub".

The SSH connection is established by using an SSH-key which is stored locally. The SSH-key must be configured by admin as it is not pre-defined on the device.

Two option are possible, when an SSH-key is stored on the device. Either the key is used solely for the SSH-connection ("Connection Key"), or the key is also used for login ("Direct Login Key").

NOTE: If a SSH-key is stored on the device, it will always be used for SSH-connection setup.

Direct Login Key

The SSH-key is used for SSH-connection as well as for CLI login. As soon as the key is verified and the access is granted, the SSH-connection is established and the login to the CLI is done. No further inquiry is needed.

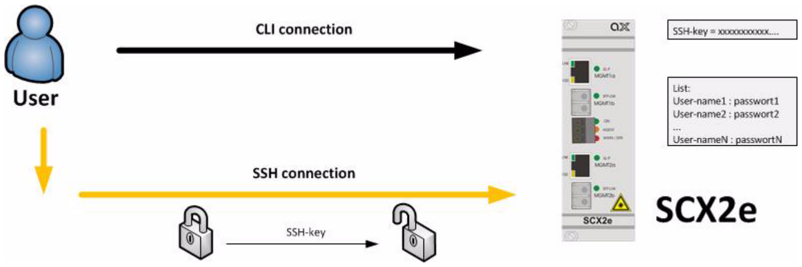


Figure 7-4 *SSH-connection using SSH-Key (Direct Login)*

Connection Key

The SSH-key is solely used to establish the SSH-connection. After successful SSH-setup, the user is asked for his login data (user-name and password). The user's login data may be locally stored and/or on a NAS. See chapter "User Administration" on page 4-36 for defining local users and usage of TACACS+.

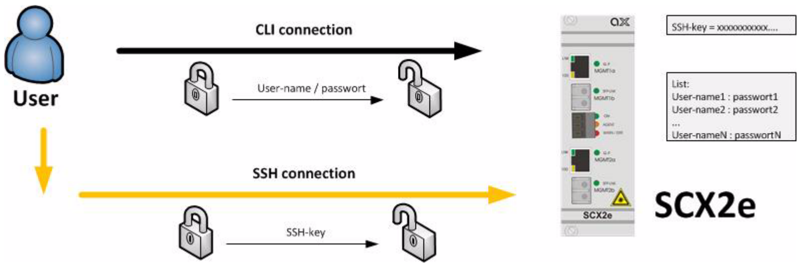


Figure 7-5 *SSH-connection using SSH-Key (Connection Key)*

Security Issues

The SSH/CLI is accessible via any TCP/IP link to the device, so it might be that other persons than the intended ones get connection and will see the login prompt. To avoid forbidden configuration or burglary of information, the access is protected against intruders via username and password.

Any time you connect or reconnect to the initialized SCX2e the login-window is displayed and a password request turns up on the terminal.

Be careful with passwords! If you write them down, keep them in a safe place. Do not choose strings easy to hack. In particular, do not use the default strings which were valid when you received the device.

Do not forget your password. If you forget your password the device will be rendered useless and will have to be sent back to the factory for basic re-configuration.

NOTE: Three different access-level are selectable with different access rights:

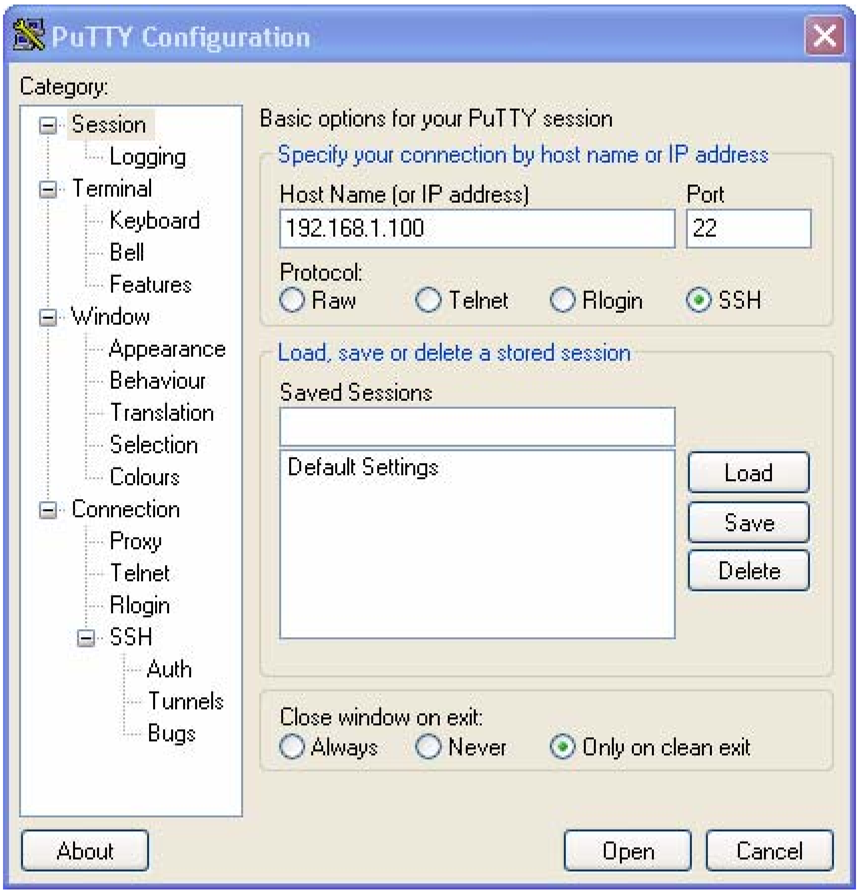
1. Guest (only view)
2. User (view and modify)
3. Admin (full access inclusive user administration)

If the device is started-up the very first time, only the user “admin” is defined. See in “User & Access Administration” on page 4-2, how to define the other users and how to change the user password.

SSH Client

There are many SSH client-SW on market, which are mainly freeware. We at arcutronix use normally the putty-SSH client and or the TeraTerm. All the following examples are related to puTTY-SSH and/or TeraTerm-SSH.

To connect to the SCX2e SSH-server establish a link via TCP/IP:



PuTTY Configuration

Basic options for your PuTTY session

Specify your connection by host name or IP address

Host Name (or IP address): 192.168.1.100

Port: 22

Protocol: ○ Raw ○ Telnet ○ Rlogin ● SSH

Load, save or delete a stored session

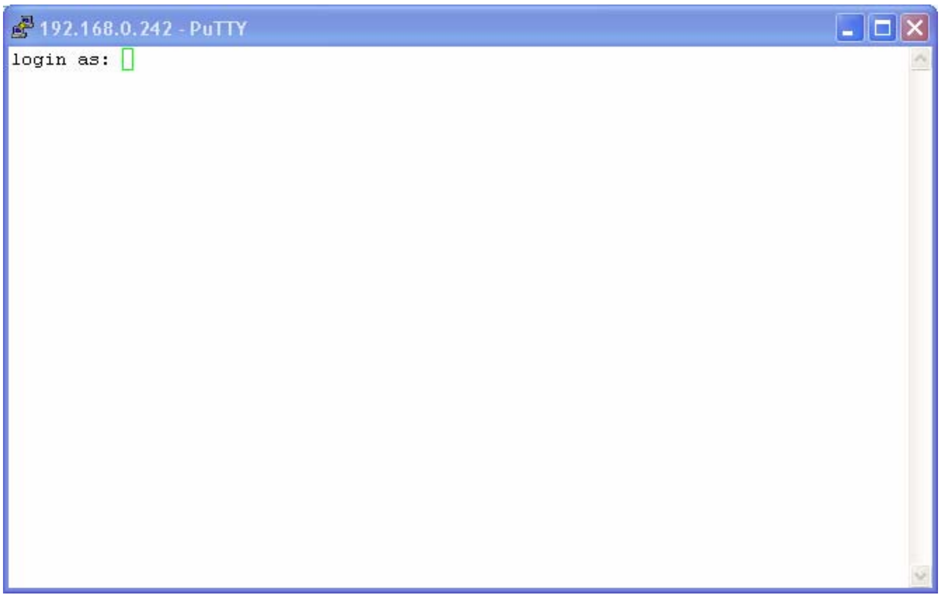
Saved Sessions: Default Settings

Close window on exit: ○ Always ○ Never ● Only on clean exit

Figure 7-6 *PuTTY SSH-Connection*

NOTE: Please make the shell-window at least 200 wide, otherwise some help-messages could be corrupted when shown.

After pressing “Open”, the Secure Shell will be opened and a prompt is visible.



```
login as:
```

Figure 7-7 Secure Shell

Now enter the user-name, which shall be used for the communication (e.g. admin) and enter the password (e.g. private).

The next message is “`Welcome <username>!`” and the connection is established.

Command Line Interface (CLI)

Introduction to the CLI

Many devices that come with support for CLI provide a huge number of different commands to configure the various functions of the device. All of these commands come with their own syntax and parameters. The CLI of arcutronix devices follows a different and more intuitive approach.

In contrast to the devices mentioned before, the CLI of arcutronix devices provides direct access to configurable parameters and device properties, so-called variables, which can be read-only (e.g. for fixed device properties) or modifiable (for configurable parameters).

Since there is a vast number of those variables, they are organized in a hierarchical menu structure. The menu structure and the ordering of information therein is logically aligned with the device functions. Once familiar with the layout of the menu structure, which is easily comprehensible, the user quickly and intuitively navigates through the menu structure and easily manipulates the device settings as needed. The CLI supports this further by giving context-sensitive help as well as automatic command and parameter completion where ever possible.

As a result, only a single command is needed to configure all aspects of the device and its functions: the “config” command explained later. It provides everything that is needed to navigate through the menu structure, to look at the information provided in submenus and to manipulate the value of configurable parameters. Each item in the menu structure (submenus, variables and possible variable values) may have helpful descriptions associated with them that can be viewed with the “config” command as well.

The navigation through the menu structure is designed to follow a principle that every computer user knows: it closely resembles the navigation though a file system. Here, menus and submenus represent directories on the hard drive, whereas configurable parameters are similar to files on the disk. The “config” command supports full path names in every place where the name of an item in the menu structure is expected. Those path names can either be relative to the current position in the menu tree, or be a path starting from the root of the menu structure. Path names are formed like file names by concatenating menu, submenu and variable names with a directory separator, for which the UNIX-style forward slash “/” was chosen. The usual name “..” for the parent menu is supported as well.

This file system similarity is also applied to more complex elements of the menu structure. For tables, which do naturally occur if there is more than one instance of an equivalent hardware component or software function present, each table row is translated into a submenu where the table columns are presented as scalar variables. Within the submenu representing the table row, editable columns can be modified as usual and further submenus of the table row become available.

Usually, the manipulation of a variable will have an immediate effect. Once the new variable value is successfully submitted, the device will make immediate use of the changed value and adjust its operation to it. Occasionally, there are cases where a group of variables needs to be consistently changed as a whole. These variable groups are also translated into submenus called “Form Pages”. Whenever the user navigates to such a form page, the CLI starts a new transaction that is automatically aborted when the user navigates away. Changes to variables within the form page will not immediately be activated but become part of the transaction data. Each form group has a BUTTON variable that fulfils the task of submitting the data and activating the changes.

CLI Editor Features

Context Sensitive Help

SCX2e-CLI offers context sensitive help. This is a useful tool for a new user because at any time during an SSH-session, a user can type a question mark (?) to get help. Two types of context sensitive help are available - word help and command syntax help.

Word help can be used to obtain a list of commands that begin with a particular character sequence. To use word help, type in the characters in question followed immediately by the question mark (?). Do not include a space before the question mark. The router will then display a list of commands that start with the characters that were entered.

Command syntax help can be used to obtain a list of command, keyword, or argument options that are available based on the syntax the user has already entered. To use command syntax help, enter a question mark (?) in the place of a keyword or argument. Include a space before the question mark. The router will then display a list of available command options with <cr> standing for carriage return.

Command Syntax Check

If a command or path is entered improperly (e.g. typo or invalid path/command option), the CLI will inform the user and indicate where the error has occurred.

NOTE: The CLI is case-sensitive in matters of the commands!

Path & Command Completion

Commands and path-entry can be completed with <TAB> to make entry quicker. When the so far entered entry is definite, the entry will be completed by pressing <TAB>. If the entry is ambiguous, the possible completion is displayed after pressing <TAB>.

For example, you can abbreviate the “config” command to “c<TAB>” because “config” is the only command that begins with “c” and the <TAB> will complete it.

NOTE: While the CLI is case-sensitive in matters of command entry, the path and variable entry is independent of the case.

Reduced Entry of Path & Command

Commands and path-entry can be abbreviated as long as the entry is definite. This is helpful when typing CLI scripts, where the auto-completion feature (with <TAB>, see above) is not available.

For example, the path “/General System Information/Inventory” can be reduced to “/G/I”.

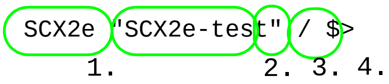
NOTE: The CLI is case-sensitive in matters of the commands!

Prompt and Path

The prompt of the CLI is built by 4 sections, which are added in the following sequence:

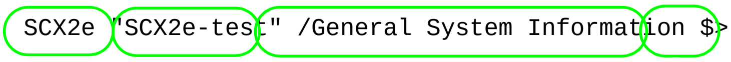
1. Device Type = SCX2e,
2. Device Name = “SCX2e” by default. The device name can be changed,
3. Path = the actual location within the menu-tree,
4. Explicit end = $>

Examples: After login, you reach the root-directory and the prompt is:



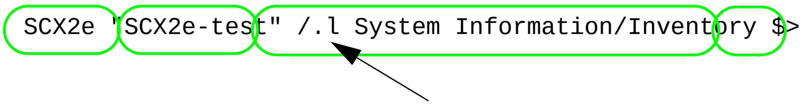
```
SCX2e "SCX2e-test" / $>
    1.         2. 3. 4.
```

After navigating to the submenu “General System Information”, the prompt will be:



```
SCX2e "SCX2e-test" /General System Information $>
```

To avoid problems with some CLI and SSH-clients, the path-statement is limited to 30 characters. If the path-statement is longer than 30 characters, the leading characters are all replaced by one dot. So after navigating to the submenu “Inventory”, the prompt will look like this:



```
SCX2e "SCX2e-test" /.l System Information/Inventory $>
```

The complete path can always be checked by the “config path” command, which prompts the actual submenu and the path from the root directory.

Comment

The CLI offers the possibility to write scripts to automate configuration and reproduce settings easily. In scripts it is worth to add comments for better understanding. A CLI comment can be written by adding a hash-symbol (#) in front of the comment. The comment may start at the beginning of a line are at any position. All text following the # will be treated as comment.

Hot Keys

For many editing functions, the SCX2e-CLI editor provides hot keys. Table 7-1 lists some editing shortcuts that are available.

Table 7-1 *SCX2e CLI Hot Keys*

Hot Key	Description
Delete	Removes one character to the right of the cursor.
Backspace	Removes one character to the left of the cursor.
TAB	Completes a partial command.
Ctrl-A	Moves the cursor to the beginning of the current line.
Ctrl-B	Moves the cursor one word to the left.
Ctrl-D	Removes one character to the right of the cursor.
Ctrl-I	Finishes a partial command.
Ctrl-J	Repeats the last command.
Ctrl-H	Removes one character to the left of the cursor.

Table 7-1 SCX2e CLI Hot Keys (continued)

Hot Key	Description
Ctrl-N	Erases a line.
Ctrl-M	<CR>.
Up Arrow	Allows user to scroll forward through former commands.
Down Arrow	Allows user to scroll backward through former commands.

NOTE: The most helpful Hot-Key is the TAB. It allows inexperienced users to complete commands, gives correct syntax and shows possible entries at all stages!

CLI Commands

Once an SSH-session is established, one can navigate within SCX2e-CLI like in a hierarchically structured tree. Command options and applications vary depending on position within this hierarchy.

To assist users in navigation through SCX2e-CLI, the command prompt will change to reflect the position of a user within the command hierarchy. This allows users to easily identify where within the command structure they are at any given moment. Also a <Tab> shows all possible options at the given position. This gives easy possibility to identify “Tab-by-Tab” the correct command.

NOTE: A <blanc> inside a string must be preceded by a back-slash (\) or the string must be wrapped by quotes. E.g.

```
$> mode “Rack View”       or
$> mode Rack\ View
```

The “Tab-by-Tab”-feature helps here a lot to build always the correct syntax.

Table 7-2 and Table 7-3 show a summary of commands and the corresponding syntax.

Table 7-2 CLI Command CONFIG

Command CONFIG	Syntax / Explanation
Summary:	
config shows or changes configuration settings. Configurations are grouped and this command can also be used to display/change configuration menu. Without an argument ***config*** shows the current configuration menu and its settings/submenus. For more details see “The command CONFIG” on page 7-15. 8 optional syntax flavours are defined:	

Table 7-2 CLI Command CONFIG (continued)

Command CONFIG	Syntax / Explanation
config	config
	Shows all the content of the current configuration submenu. The first character in each row indicates the type of variable that is shown: • > for submenus, • F for form pages, • * for read-writeable variables, • ! for read-writeable password variables, • + for executable commands, • (blank) for read-only variables. Options: none
config path	config path
	Shows the complete path of the current configuration page. As the CLI's prompt does only show a reduced path (30 characters), it might be helpful to see the complete path for verification. Options: none
config go	config go <PATH>
	Changes to a different configuration page. Options: • <PATH> = root: topmost menu • <PATH> = up: go to parent menu • otherwise: go to submenu identified by PATH. The PATH may start at the present submenu or at root (/). Suitable submenus are identified by: • > (regular submenu) • F (form page)
config VARIABLE	config [PATH\]VARIABLE
	Display the current value of VARIABLE. Options: • <PATH>: path to VARIABLE in submenu identified by PATH. The PATH may start at the present submenu or at root (/). If empty, VARIABLE must exists in the current submenu. Suitable submenus are identified by: • * (read-write) • ! (read-write password) • (blank: read-only) • VARIABLE: management variable to be displayed.

Table 7-2 CLI Command CONFIG (continued)

Command CONFIG	Syntax / Explanation
config help	config help [PATH\]VARIABLE
	Display help-information for VARIABLE. Options: • PATH: path to VARIABLE in submenu identified by PATH. The PATH may start at the present submenu or at root (/). • VARIABLE: management variable. Allowed are all items that the config command displays.
config set	config set [PATH\]VARIABLE VALUE
	Change the value of VARIABLE to new VALUE. Options: • PATH: path to VARIABLE in submenu identified by PATH. The PATH may start at the present submenu or at root (/). • VARIABLE: management variable to be modified. Allowed are variables identified by: • * (read-write) • ! (read-write password) • VALUE: New value of the variable. Value must be according the defined value range of VARIABLE.
config hidden	config hidden [PATH\]VARIABLE
	Change the value of the protected (password) VARIABLE in a hidden mode. The password will be prompted for in a new line. The typed value will be invisible for security reasons. To protect from accidentally mistyping errors, the new value has to be re-entered for confirmation. Options: • PATH: path to VARIABLE in submenu identified by PATH. The PATH may start at the present submenu or at root (/). • VARIABLE: A special protected (password) VARIABLE. Allowed are variables identified by: • ! (read-write password)
config do	config do [PATH\]COMMAND
	Start or execute COMMAND. Options: • PATH: path to VARIABLE in submenu identified by PATH. The PATH may start at the present submenu or at root (/). • COMMAND: A command starts a complex action. Allowed are variables identified by: • + (executable command)

Table 7-3 All other *CLI Commands*

Command	Syntax / Explanation
help	help [COMMAND | Short-cut]
	help without any further entry shows all the commands and short-cuts, which are available. When help followed by a command or short-cut, the detailed help-text for it will be presented. For help an alias is available: ? help is in any context available. • ARG COMMAND - any available command.
log	log [LINES]
	Show last entries of the log file. The optional parameter allows to specify the number of lines to show. • ARG LINES - The number of lines to print at most (default: 100).
quit	quit
	Quit the current CLI session.
show	show [<PATH>]
	Displays the settings in the selected (or current) menu in a format suitable for copying the lines back into the CLI. Changeable settings are printed as CLI commands, read-only settings are printed as comments. Each line is terminated by a semi-colon. ARG PATH - Path to a menu. If omitted, current menu-path is used.
showall	showall [<PATH>]
	Displays the settings in the selected (or current) menu including all submenus in a format suitable for copying the lines back into the CLI. Changeable settings are printed as CLI commands, read-only settings are printed as comments. Each line is terminated by a semi-colon. ARG PATH - Path to a menu. If omitted, current menu-path is used.
cards	cards
	Displays basic rack (fan, power supply, etc.) information and all line cards currently accessible to the agent, ordered by their position inside the rack. Remote line cards are shown below the in-rack line card that they are connected to.

Table 7-3 All other *CLI Commands (continued)*

Command	Syntax / Explanation
select	select <card specification>
	Selects a different line card or agent for configuration. There are different possibilities to specify the card to select: • select agent selects the agent card • select [rack <RACK>] slot <SLOT> selects the line card in the rack named <RACK> and slot number <SLOT> • select serial <SERIAL> selects the line card with serial number <SERIAL> • select <DEVICENAME> selects the line card that is named <DEVICENAME> After the new card has been selected, the menu tree will be replaced with a different menu tree that reflects the configuration capabilities of the selected line card.

The command CONFIG

The command CONFIG is the most mighty tool in the SCX2e CLI. It is only available in Cardview-mode and gives access to the menu-structure of the selected card. The menu-structure of the individual card-types can vary. Please refer to the individual manuals of the different cards to get more information on the different menu-structures.

Within this document, the following examples will mostly depend on the SCX2e itself. For complete overview to all variables see additional document [axRefGuideCLI_SCX2e].

When entering the command CONFIG apart in any context (of the Cardview-mode), the available menu-entries are shown:

```
Agent SCX2e "Main Agent" / $> config
--Login
> General System Information
> Administration
> Alarm Management
> Firmware Update
```

The first 1-2 signs in the resulting overview are type-indicators which shows what can be done with this entry and which `config`-command can be used.

Table 7-4 Menu Indicators and corresponding CONFIG Commands

Type	Explanations / Examples

--	Headline:
	This is the name of the shown menu. Nothing can be done with CONFIG; it is only a text.
	Example:
	`$> config`
	`--LOGIN`
	`.`
	`.`
	`$>`

>	Submenu:
	“>“ indicates a submenu, which can be accessed via
	CONFIG GO <submenu-name>
	Example:
	`$> config`
	`--Login`
	`> General System Information`
	`> Administration`
	`> Alarm Management`
	`> Firmware Update`
	`$> config go Administration`
	`/Administration $>`

*	Changeable Management Variable
	“*“ indicates a menu-entry which can be changed via
	CONFIG SET <variable-name> <value>
	Example:
	`/General System Information $> config`
	`--General System Information`
	`* Device Name: “ENX-F”`
	`.`
	`.`
	`.`
	`/General System Information $> config set Device\ Name “New Name”`
	`/General System Information $> config`
	`--General System Information`
	`* Device Name: “New Name”`
	`.`
	`.`
	`.`
	`/General System Information $>`

Table 7-4 *Menu Indicators and corresponding CONFIG Commands (continued)*

!

Password or other sensitive data. This variable should be configured with care. When entering a new value for the variable and the configuration can be done in “hidden” mode.

“!“ indicates a menu-entry which can be changed in hidden mode (with double entry for verification) or standard mode (with single entry and the entry is readable).

CONFIG HIDDEN <variable-name> or

CONFIG SET <variable-name> <value>

Examples:

By hidden command (config hidden):

```
..Modify Account/Change Password $> config
-- Modify Account
! Password: <hidden>
+ [Change Password]
  Form data will only be submitted after executing 'config do
Change Password'
..Modify Account/Change Password $> config hidden Password
Enter password:
Retype password:
..Modify Account/Change Password $> config do Change\ Password
Really change the Password (y/n)?
Proceed? [yes|no] $> y
Data submitted.
..Modify Account/Change Password $>
```

or by standard config set command:

```
..Modify Account/Change Password $> config
-- Modify Account
! Password: <hidden>
+ [Change Password]
  Form data will only be submitted after executing 'config do
Change Password'
..Modify Account/Change Password $> config set Password Ne1wPw_
..Modify Account/Change Password $> config do Change\ Password
Really change the Password (y/n)?
Proceed? [yes|no] $> y
Data submitted.
..Modify Account/Change Password $>
```

+

Command

“+“ indicates a command-entry which can be invoked via

CONFIG DO <command-name>

Example:

Table 7-4 Menu Indicators and corresponding CONFIG Commands (continued)

	`/Administration/Reset System $> config`
	`--Reset System`
	`  Reset State: No reset scheduled`
	`* Reset Mode: Immediate reset`
	`+ [Start Reset]`
	`/Administration/Reset System $> config do Start\ Reset`

blanc	Read-Only Variable
	No sign (or blanc character “ “) indicates a read-only variable which can be read via
	CONFIG <variable-name>
	Example:
	`/General System Information $> config`
	`--General System Information`
	`.`
	`.`
	`.`
	`Device Temperature: “35.5”`
	`.`
	`/General System Information $> config Device\ Temperature`
	`“35.5”`
	`/General System Information $>`

There are some special CONFIG commands, which help to navigate:

Table 7-5 Special CONFIG Commands

Type	Explanations / Examples

	Go back one directory in the directory-tree of the selected device in Cardview-mode.
	Example:
	`/Administration/Reset System $> config go up`
	`/Administration $> config go up`
	`$>`

	Goto root directory of the selected device in Cardview-mode.
	Example:
	`/Administration/Reset System $> config go root`
	`$>`

Quick Usage Guide for CLI-Commands

Table 7-6 CLI Quick Reference

Show options in actual menu: `$> config`

Change Contact Person: [General System Information -> Contact Person]
`$> config go General\ System\ Information`
`$> config set Contact\ Person “new Name”`

Reboot Device: [Administration -> Reset System]
`$> config go Administration`
`$> config go Reset\ System`
`$> config set Reset\ Mode Immediate\ Reset`
`$> config do Start\ Reset`

Go back 1 Step in Menu: `$> config go up`

Go back to Top-Level Menu (/):
`$> config go root`

Show the complete path (remember, the path within the prompt is limited to 30 characters): `$> config path`

Example for SSH-Script

TeraTerm and other SSH-clients are supporting scripting to execute commands in always the same way. In the following, a short example for an TeraTerm-script is given to show the initial setup to a host and how to enter some simple commands.

The script will do the following:

1. Connect to the device (192.168.1.100) with user-name “admin” and password “private” using SSH2
2. Change the contact person’s name to “Miss Marple”,
3. Change the units name to “test-unit with new name”,
4. Disconnects the session.

Table 7-7 *Example for SSH-Script*

Step	Code

0	`;;  Tera Term Macro`
	`;;  ========================================================================`
	`;;  file    __prog_SCX2e.ttl`
	`;;`
	`;;  desc    Example for Teraterm programming-file.`
	`;;  ========================================================================`
	`;;  HISTORY`
	`;;`
	`;;  2011-02-21 arcutronix GmbH        Initial Version`
	`;;`
	`;;  ========================================================================`

1	`;; open Tera Term`
	`;;`
	`connect '192.168.1.100 /SSH /2 /auth=password /user=admin /passwd=private`

2	`wait '/ $> '`
	`sendln 'config go “General System Information”'`
	`wait ’ $>’`
	`sendln ’config set “Contact Person” “Miss Marple”’`
	
	`3     wait ’ $>’`
	`sendln ’config go “General System Information”’`
	`wait ’ $>’`
	`sendln ’config set "Device Name" "test-unit with new name"’`

4	`pause 1`
	`disconnect 0`
	`end`

Appendix A
Technical Specifications

SCX2e Hardware Specification

Hardware & Power

Table A-1 to Table A-8 provide the general technical data of the SCX2e - System Controller.

Table A-1 Mechanic and Environment

Type	
Mechanics	
Design:	AgentCard for rack-mount chassis or desktop housing
Dimensions:	190 x 130 x 30mm
Weight:	180g
Environmental Conditions	
Operation:	ETSI ETS 300 019-1-3, class 3.1E
Temperature (hardened version) Humidity	-5 ... +55 °C 10 ... 90%, non-cond.
Storage (in packing)	ETSI ETS 300 019-1-1, class 1.2
Temperature Humidity	-25 ... +55 °C 10 ... 100%, non-cond.
Transportation:	ETSI ETS 300 019-1-2, class2.3
Temperature Humidity	-40 ... +70 °C 10 ... 95%, non-cond.

Table A-1 Mechanic and Environment (continued)

Type	
Others	
Ingress Protection:	IP30
DIN EN 60529 (VDE 0470 Part 1)	
Fan:	none
Cooling:	Convection cooling through ventilation slots in the housing environment

Table A-2 Security and EMC

SCX2e-Family	SCX2e
EMC	
	EN 55022:1998 + A1:2000 class B
	EN 61000-3-2:2000
	EN 61000-3-3:1995 + A1:2001
Product Security	
Electrical security:	EN 60950
Sound emission:	None (no build-in fan)
Conformity:	CE

Table A-3 Power Requirements

Type			
Power Supply			
Type:	DC		
Input voltage:	+5VDC	+/- 5%	
Connector:	Via backplane		
Power Requirements [i]			
Device	w/o SFP(s)	With Standard SFP(s) (700mW)	Max. power to be used by SFP(s)
SCX2e	4.0 VA	4.7 VA (1x SFP)	1.8 VA

Table A-3 Power Requirements (continued)

Type			
SCX2e-WDM	4.0 VA	4.7 VA (1x SFP)	1.8 VA

i. The total power need depends on the used SFP(s).

Interfaces

Table A-4 Number of Interfaces

Type		
SCX2e-Family		
Number of Interfaces		
SCX2e	2x Gigabit Ethernet 10/100/1000BaseT (RJ45),	General Purpose
	2x Gigabit Ethernet 1000BaseFX/TX (SFP),	General Purpose
	1x Alarm Connector	NOC (normal open)
SCX2e-WDM	1x Gigabit Ethernet 10/100/1000BaseT (RJ45),	Local Management-I/F,
	1x Gigabit Ethernet 1000BaseFX/TX (SFP),	Remote Management-I/F,
	1x Gigabit Ethernet 1000BaseFX/TX (SFP),	ax-internal Management-I/F via WDM,
	1x passive WDM-Filter (1310 + 1550nm, SM, SC-connector),	Overlay network for remote Management,
	1x Alarm Connector	NOC (normal open)

Table A-5 Technical Data of the Interfaces

Type	
Interfaces	
Fast Ethernet Interfaces (Copper)	
Type:	IEEE 802.3 (full- and half-duplex, Autonegotiation)
Data-rate	10 or 100Mbps

Table A-5 Technical Data of the Interfaces (continued)

Type	
Connection type:	Twisted-Pair interface (TP)
Function, electrical values, pin assignment:	according to IEEE 802.3i (10BaseT), IEEE 802.3u (100BaseTX)
Impedance:	100 Ohm (balanced)
Connector:	8 pin RJ45 connector according to ISO 8877
Fast Ethernet Interfaces (SFP)	
Type:	IEEE 802.3 (full- and half-duplex, Autonegotiation)
Connection type:	Fibre Optics (FO), SFP
Function, electrical values:	IEEE 802.3u (100BaseFX, 100BaseSX, 100Base-BX, 100Base-LX10)
Connector:	LC
SFP:	According to SFP MSA, Rev 4.5, Aug. 31, 2006 All vendors supported. Max. 100 insertion / extraction.
Gigabit Ethernet Interface (Copper)	
Type:	IEEE 802.3 (full- and half-duplex, Autonegotiation)
Connection type:	Twisted-Pair interface (TP)
Function, electrical values:	according to IEEE 802.3i (10BaseT), IEEE 802.3u (100BaseT) IEEE 802.3ab (1000BaseT)
Impedance:	100 Ohm (balanced)
Connector:	8 pin RJ45 connector according to ISO 8877
Gigabit Ethernet Interface (SFP)	
Type:	IEEE 802.3 (full-duplex)
Connection type:	Fibre Optics (FO), SFP
Function, electrical values:	IEEE 802.3z (1000Base-X
Connector:	LC or RJ45
SFP:	According to SFP MSA, Rev 4.5, Aug. 31, 2006 All vendors supported. Max. 100 insertion / extraction.

Table A-5 Technical Data of the Interfaces (continued)

Type	
Alarm Connector	
Alarm Connector:	RIA (3 pin)

Table A-6 WDM-Filter

Type	
WDM-Filter	
Connector	LC/PC
Max. Insertion Loss (dB)	0.3
Min. Isolation (dB)	17
Polarization Stability (dB)	0.1
Bandwidth (nm)	+/- 15
Directivity (dB)	>55
Temp. Coefficient (dB/)	0.002

µController, Display & Clock

Table A-7 Display Functions

Type	
Display Functions	
System:	3 LEDs for system, operating and error status
Copper Gigabit Ethernet interfaces:	2 LEDs each, for Link Status, Activity and 10/100/1000Mbps recognition (only TP ports)
Fibre Gigabit Ethernet interfaces:	1 LED each, for Link Status and Activity

Table A-8 µController and Clock

Type	
Electronics	
Main processor:	32 Bit power PC, Freescale MPC8313E
Non-volatile memory:	64 MB
Main memory:	128 MB SDRAM
Real Time Clock	
Accuracy	10ppm (<1sec/day)
Hold Time (without ext. power)	min. 11 days

SCX2e Software Specification

Table A-9 provides the general technical data of theSCX2e - System Controller.

Table A-9 Technical Data of the SCX2e- Software

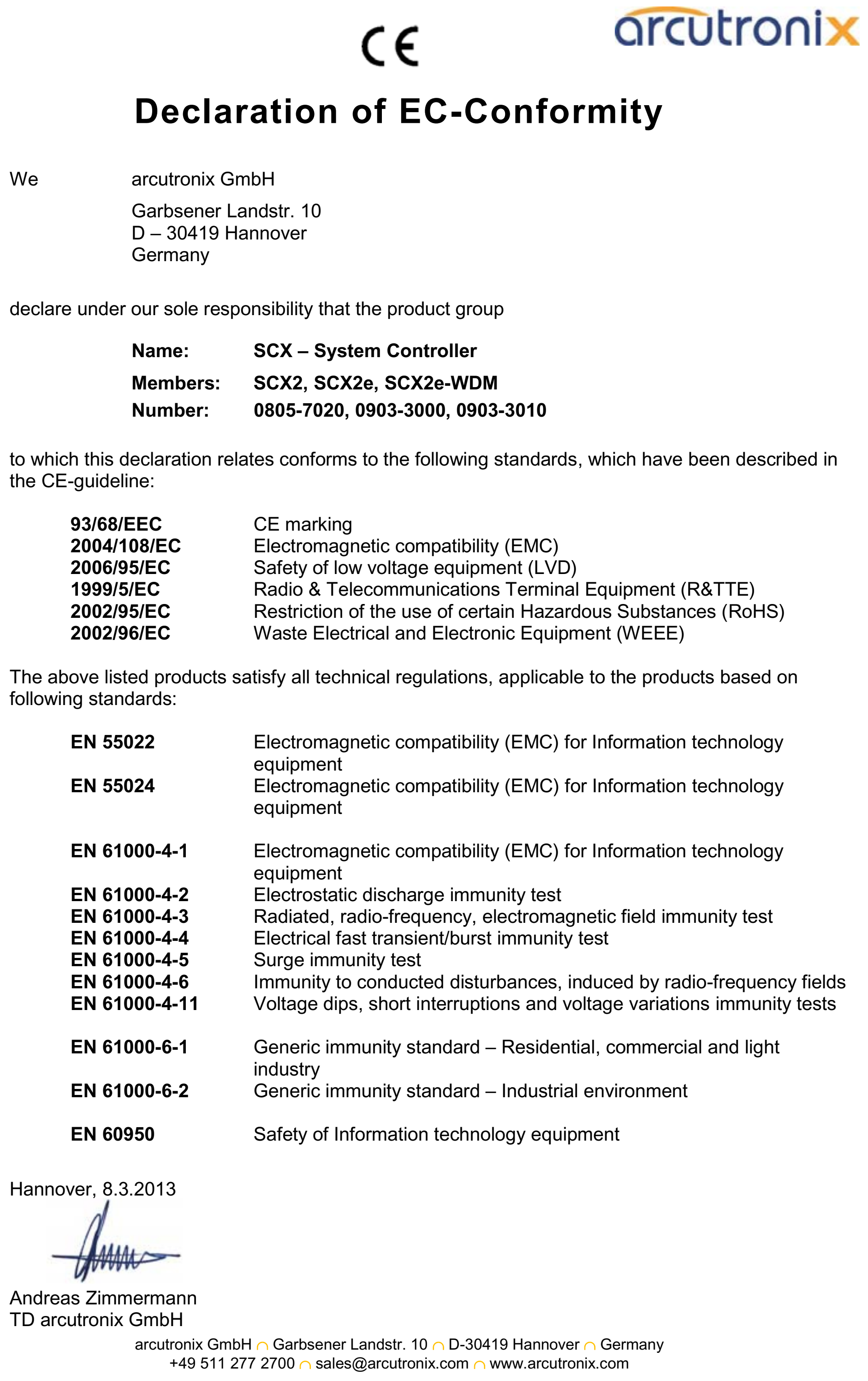
Type		
SCX2e		
General Information		
Valid SW-Version for this manual:	V 2_0_01 [i]	
Standards		
Internet Protocol:	IPv4	
	IPv6	
IP-address assignment:	manually	
	DHCP	RFC 2131
	IPv6 Auto-Conf	RFC 2462
SNMP:	SNMPv2c	RFC 1901, RFC 1905, RFC 1906
	SNMPv3	IETF RFC 3410 - RFC 3418
	SNMPv2-MIB	RFC 3418
	RMON MIB (rmon1, rmon2, rmon3, rmon4 and rmon9)	
	IF-MIB	RFC 2863
Secure Shell (SSH)	SSHv1	draft-ylonen-ssh-protocol-00.txt
	SSHv2	RFC 4250 - RFC 5256
TFTP		RFC 1350
SFTP		draft-ietf-secsh-filexfer-02.txt
http	http /1.1	RFC 2616

[i] If you use higher SW-version, please check with arcutronix or your local partner, whether there is a new release of the manual available.

Table A-10 Management & Security

SCX2e-Family	SCX2e	SCX2e-WDM
HTTP server	yes	yes
HTTPS server	yes	
CLI (via SSH)	yes	yes
Web and CLI authentication and authorization	yes	yes
Software download through Web	yes	yes
Software download through FTP	yes	yes
Configuration download or upload	yes	yes
SNMPv2c/v3Agent	yes	yes
TACACS+	yes	yes

Appendix EC
EC Declaration of Conformity



Declaration of EC-Conformity

We arcutronix GmbH

Garbsener Landstr. 10
D – 30419 Hannover
Germany

declare under our sole responsibility that the product group

Name:	**SCX – System Controller**
Members:	**SCX2, SCX2e, SCX2e-WDM**
Number:	**0805-7020, 0903-3000, 0903-3010**

to which this declaration relates conforms to the following standards, which have been described in the CE-guideline:

93/68/EEC	CE marking
2004/108/EC	Electromagnetic compatibility (EMC)
2006/95/EC	Safety of low voltage equipment (LVD)
1999/5/EC	Radio & Telecommunications Terminal Equipment (R&TTE)
2002/95/EC	Restriction of the use of certain Hazardous Substances (RoHS)
2002/96/EC	Waste Electrical and Electronic Equipment (WEEE)

The above listed products satisfy all technical regulations, applicable to the products based on following standards:

EN 55022	Electromagnetic compatibility (EMC) for Information technology equipment
EN 55024	Electromagnetic compatibility (EMC) for Information technology equipment
EN 61000-4-1	Electromagnetic compatibility (EMC) for Information technology equipment
EN 61000-4-2	Electrostatic discharge immunity test
EN 61000-4-3	Radiated, radio-frequency, electromagnetic field immunity test
EN 61000-4-4	Electrical fast transient/burst immunity test
EN 61000-4-5	Surge immunity test
EN 61000-4-6	Immunity to conducted disturbances, induced by radio-frequency fields
EN 61000-4-11	Voltage dips, short interruptions and voltage variations immunity tests
EN 61000-6-1	Generic immunity standard – Residential, commercial and light industry
EN 61000-6-2	Generic immunity standard – Industrial environment
EN 60950	Safety of Information technology equipment

Hannover, 8.3.2013

Andreas Zimmermann
TD arcutronix GmbH

arcutronix GmbH ∩ Garbsener Landstr. 10 ∩ D-30419 Hannover ∩ Germany
+49 511 277 2700 ∩ sales@arcutronix.com ∩ www.arcutronix.com

Headquarter

arcutronix GmbH
Garbsener Landstrasse 10
30419 Hannover
Germany

Phone:	**+49 (511) 277 2700**
Fax:	**+49 (511) 277 2709**
Email:	**info@arcutronix.com**
Web:	**www.arcutronix.com**