PRAESENSA

Public Address and Voice Alarm System

en Instructions for Maritime Cyber Security

Table of contents

1	**Introduction**	**5**
1.1	Safety and security information	5
2	**Asset inventory**	**7**
2.1	General information	7
2.1.1	Additional service tools	7
2.2	Core devices	7
2.2.1	System controller	7
2.2.2	Call stations	8
2.2.2.1	Call station	8
2.2.2.2	Call station extension	9
2.2.3	Multifunction power supply	9
2.2.4	Amplifier	10
2.2.5	Control interface module	10
2.2.6	Audio interface module	11
2.2.7	Ambient noise sensor	11
2.2.8	Wall control panel	12
2.2.9	OMNEO to Dante gateway	13
2.3	Core applications	13
2.3.1	PRAESENSA Logging applications	13
2.3.2	PRAESENSA Network Configurator	13
2.4	Network equipment	14
2.4.1	Fiber transceiver	14
2.4.2	Ethernet switch	14
3	**Communication protocols and ports**	**15**
3.1	CAP2	15
3.1.1	Supported protocols	15
3.1.2	Port usage	15
3.2	CAP6	17
3.2.1	Supported protocols	17
3.2.2	Port usage	17
3.3	System controller	19
3.3.1	Device part - Supported protocols	19
3.3.2	Device part - Port usage	19
3.3.3	Controller part - Supported protocols	19
3.3.4	Controller part - Port usage	20
3.4	Call station	23
3.4.1	Supported protocols	23
3.4.2	Port usage	23
3.5	Amplifier	24
3.5.1	Supported protocols	24
3.5.2	Port usage	24
3.6	Multifunction power supply / Audio interface module	24
3.6.1	Supported protocols	24
3.6.2	Port usage	25
3.7	Ambient noise sensor / Control interface module / Wall control panel	25
3.7.1	Supported protocols	25
3.7.2	Port usage	25
3.8	Ethernet switch	26

3.8.1	Supported protocols	26
3.8.2	Port usage	26
3.9	Logging applications	27
3.9.1	Supported protocols	27
3.9.2	Port usage	27
4	**Security functionality verification**	**28**
4.1	System controller configuration	28
4.2	Logging applications	28
4.3	Ethernet switch	29
4.4	Installation	29
4.5	Firewall configuration rules	29
5	**Configuration guidelines**	**31**
5.1	Open interface protocol	31
5.2	Passwords usage	31
6	**System topologies**	**32**
6.1	Logical topology	32
6.2	Physical topology	33
7	**Incident response plan**	**34**
7.1	Forensics by use of audit records	34
7.2	Controlled shutdown, reset, roll-back and restart	34
8	**Other supporting documentation**	**35**
9	**Checklist**	**36**

1 Introduction

The **Instructions for Maritime Cybersecurity** describes the design and operation of the Electro Voice Dynacord PRAESENSA Public Address and Voice Alarm system, including the individual PRAESENSA devices that can be used in standalone or networked configurations.

PRAESENSA is an IP-network based Public Address and General Alarm (PA/GA) system. Based on OMNEO audio as encrypted Dante, it distributes audio from one or more sources to one or more destinations with multicast messaging. This can be used to distribute:

- Announcements with live voice audio from a call station through the amplifiers to the loudspeakers.
- Prerecorded messages and attention or alarm tones to the loudspeakers.

Background music is distributed in a similar way.

The audio distribution is based on priority: the highest priority audio us distributed in case of conflicts in the destinations. This ensures that evacuations and General Alarm calls have priority over business announcements and background music, as well as other entertainment-related audio.

The network is a redundant Gbit Ethernet network with RSTP for loop resolving. Communication between the devices is based on OMNEO OCA, which is a TLS-based secure communication protocol.

Refer to *System topologies, page 32* for topology examples.

The system consists of:

- The *System controller, page 7* maintains the connection with the other devices and controls the system.
- The *Call stations, page 8* enable announcements.
- The *Multifunction power supply, page 9* supply power from mains and backup.
- The *Amplifier, page 10* supply the 100 V audio to the loudspeakers.
- The *Control interface module, page 10* provides input and output contacts.
- The *Audio interface module, page 11* provides analog audio inputs and outputs.
- The *Ambient noise sensor, page 11* enables the control of the loudness of the audio depending on the ambient noise.
- The *Wall control panel, page 12* enable the control of the background music volume in a room.

1.1 Safety and security information

- Always use a firewall or network segmentation with third-party traffic limiting routers.
- For maximum security, install the devices in lockable racks.
  - In particular, emergency call stations must have a physical protection or be installed in a restricted area.
- To keep the Logging applications protected:
  - The Logging Server and the Logging Viewer must be installed on the same PC.
  - The PC must be physically protected.
  - The users must log in into a Windows accounts to have access to the applications.
  - The users must set a password to gain access to the Logging Server settings.
- The priority of business call stations, VoIP and Dante must be lower than the emergency priority.
- Only use secure Open Interface ports.

To keep the PRA-ES8P2S Ethernet switch protected:

- Remove the default user and use encrypted SNMPv3 communication with enabled SHA authentication protocol and AES privacy protocol for read-only access.
- Always change the initial password.
- To allow for the time-stamped events, enable NTP in the system controller and in the switch.
- Configure the switch to log into file storage, and not into buffer, to keep the logging data stored and accessible.
- In the configuration interface of the switch, in **Tools**, enable **62443 Security**.
- In the 62443 security settings of the switch, enable **Signed Firmware Upgrade**.

2 Asset inventory

2.1 General information

Version

The PRAESENSA devices and applications in the same system must have the same firmware and software version. The only exception is the call stations' extension.

The firmware can be installed and upgraded with the Firmware Upload Tool (FWUT).

Hardware type approval references

- A1519520
- A1577186

Operating systems

PRAESENSA uses the following operating systems:

- A bespoke distribution based on Yocto Scarthgap of embedded Linux for the system controller.
- FreeRTOS 9.0 for the other PRAESENSA devices.

2.1.1 Additional service tools

Configuration interface

The configuration of the PRAESENSA system is done in the configuration interface through a web-browser.

Firmware Upload Tool (FWUT)

The FWUT is used to upload the firmware of the hardware devices.

Network Configurator

The PRAESENSA Network Configurator permits the configuration of the IP-address of the network interfaces of the devices. It is possible to configure the devices for static IP-addressing or for DHCP. Refer to *PRAESENSA Network Configurator, page 13*.

OMNEO Network Docent

The OMNEO Network Docent allows the user to map and visualize the network interconnections of the PRAESENSA devices.

Dante Controller

The Dante Controller allows the user to configure and route the audio around Dante networks. This application is developed by Audinate.

2.2 Core devices

2.2.1 System controller

The system controller manages the communication between the PRAESENSA devices. The system controller is the responsible for the system control and supervision. It routes all audio connections between the audio sources and the audio destinations.

The PRAESENSA system is configured through the system controller through a configuration interface in a web-browser.

The following functions are the responsibility of the system controller:

- Device control.
- Device supervision.
- Fault and event logging.
- Priority management.
- Playing prerecorded messages though its internal message players.
- Interfacing with external applications through:
  - The Open Interface client, which allows PRAESENSA to connect to third-party applications. In the configuration, it is possible to disabled the general alarm functionality. The connection is authenticated and encrypted with TLS.
  - The Dante controller to connect external audio sources, for example for background music. The configuration in the system controller defines whether the Dante channels are distributed in the PRAESENSA system.
  - Voice Over IP to initiate calls from a telephone. VoIP calls must only be used for low-priority business announcements. The SIP interface can be connected securely.

The system controller has the following hardware characteristics:

- Five Ethernet ports internally connected to a switch.
- Dual power supply supplied from a PRA-MPS3.
- Internal message player with non-volatile storage for a large number of messages.
- Two network interfaces behind the internal switch. The controller uses two IP-addresses.
- An SD-card slot for future use, which has no current function.

The system controller can be deployed redundantly with one controller serving as the duty controller and other controllers in standby, as backup.

Two versions of the system controller are available:

- The large PRA-SCL.
- The small PRA-SCS. The PRA-SCS has the same functionalities but differs in the allowed system size and in the number of Dante audio channels.

2.2.2 Call stations

2.2.2.1 Call station

PRA-CSLD

PRA-CSLW

The call station distributes live voice messages. The call station extension provides additional buttons to select the zones (destinations) of the audio. Up to four extension devices can be connected to a call station. The functionality of the call station and of the extension buttons is configured in the configuration interface.
To prevent unauthorized access, it is possible to configure a user/pin combination.
The call station has the following hardware characteristics:
- Two Power over Ethernet (PoE) connections internally connected to a switch. These allow for:
  - Ethernet loop-through.
  - Redundant power.
  - CAN bus to connect the extensions through RJ12 connectors.
- Two network interfaces behind the internal switch. The call station uses two IP-addresses.

Two versions of the call station are available:
- The tabletop PRA-CSLD with a stem microphone.
- The wall-mount PRA-CSLW with a detachable fist microphone.

2.2.2.2 Call station extension

The PRA-CSE Call station extension has 12 buttons with indicators that extend the number of buttons for a call station. The button functionality is configured in the configuration interface. The call station extension connects to the call station through CAN bus with an RJ12 connector. This device does not run an operating system.
Use software version 2.40.

2.2.3 Multifunction power supply

The PRA-MPS3 Multifunction power supply, large can redundantly power:
- The system controller.
- Three amplifiers.
- Two PoE devices.

The primary power supply is the mains power. The secondary power supply is a 12 V battery. A charger for the backup power supply is included.
The multifunction power supply has the following hardware characteristics:

– Five copper Ethernet ports. Two of these powers supply PoE.
– One SFP slot for fiber connection.

All ports are internally connected to a switch and can be used for network interconnections of other PRAESENSA devices. Ports 1 and 2 supply PoE to power PoE devices such as the call stations.
The PRA-MPS3 has control input and output contacts. The functions are configurable through the configuration interface.
An analog lifeline to the amplifiers allows for audio routing in case the control board of the amplifier fails.

2.2.4 Amplifier

PRA-AD604 PRA-AD608

The amplifier distributes the received audio to the loudspeakers over a 100 V loudspeaker line. The amplifier has an additional redundant channel to take over a failing amplifier channel. The audio characteristics are configured in the configuration interface.
The amplifier has two copper Ethernet ports. Both ports are internally connected to a switch.
An analog lifeline to the multifunction power supply allows for audio routing in case the control board of the amplifier fails.
Two versions of the amplifier are available:
– The four channel PRA-AD604.
– The eight channel PRA-AD608.

2.2.5 Control interface module

The PRA-IM16C8 Control interface module supports:
– Sixteen supervised input contacts.

– Eight output contacts.
– Two additional supervised output contacts.

The functions for the inputs and outputs are configured in the configuration interface.
The interface module has two Power over Ethernet (PoE) connections for Ethernet loop-through and redundant power supply. Both are internally connected to a switch.

2.2.6 Audio interface module

The PRA-IM2A2 Audio interface module supports:
– Two analog or digital audio inputs and outputs.
– Two supervised input contacts.
– Two output contacts.

The functions for the inputs and outputs are configured in the configuration interface.
The interface module has two Power over Ethernet (PoE) connections for Ethernet loop-through and redundant power supply. Both are internally connected to a switch.

2.2.7 Ambient noise sensor

The PRA-ANS Ambient noise sensor adapts the distributed audio level to the actual ambient noise level in the zone. This improves speech intelligibility.
The ambient noise sensor has one Power over Ethernet (PoE) connection.

2.2.8 Wall control panel

PRA-WCP-EU PRA-WCP-US

The wall control panel adapts the background music in a zone. It has a single rotary button to select the background music source and to adapt the volume for the zone. To prevent unauthorized access, it is possible to configure a pin.
The wall control panel has one Power over Ethernet (PoE) connection,
Two versions of the wall control panel are available:

– The PRA-WCP-EU fits in the standard European round box.
– The PRA-WCP-US fits in a standard rectangular US box.

2.2.9 OMNEO to Dante gateway

The OMN-DANTEGTW Dante gateway allows the transference of audio between two independent networks. The networks are otherwise kept separate. The device receives Dante audio streams and passes them through to the PRAESENSA system controller as Dante streams.

Notice!
Only use the OMN-DANTEGTW once it is certified.

2.3 Core applications

2.3.1 PRAESENSA Logging applications

The PRAESENSA Logging applications consists of:

- The Logging Server, which collects events to store on the PC. The Logging Server connects to the system controller through the Open Interface port.
- The Logging Viewer, which allows the user to view events and acknowledge and reset fault events. The Logging Viewer connects to the Logging Server and is used through the PC.

2.3.2 PRAESENSA Network Configurator

The PRAESENSA Network Configurator is a Windows application only used during the installation of the system. It allows for setting up a PRAESENSA system with static IP-addresses.

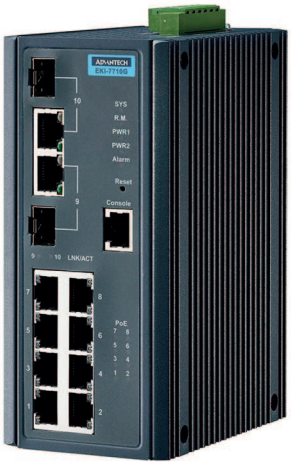
2.4 Network equipment

2.4.1 Fiber transceiver

The fiber transceiver, manufactured by Advantech, is used in combination with the multifunction power supply to make fiber connections.
Two versions of the fiber transceiver are available:

- The single mode PRA-SFPLX.
- The multimode PRA-SFPSX.

2.4.2 Ethernet switch



The PRA-ES8P2S Ethernet switch has 10 ports. Two can be used as fiber ports to connect the fiber transceivers. The switch has a dual power supply, which can come from a multifunction power supply or from other power source.
Take into account the following information about the Ethernet switch:

Version	1.03.05
Manufacturer	Advantech
References of the hardware type approval	A1519520 A1577186
Operating system	Embedded Linux

Notice!
Use only the **BE** version of the PRA-ES8P2S switch. The AE version of the switch needs a different firmware that is not compliant to UR E27.

3 Communication protocols and ports

The following overview covers the supported protocols and ports used as of the 2.20 PRAESENSA release.

3.1 CAP2

The CAP2 is a subcomponent of PRAESENSA audio devices with only two audio channels.

3.1.1 Supported protocols

Protocol	Description	Comment
AES67	AES67 audio	
ARP	Address Resolution Protocol	
Dante	Dante audio support	
DHCP	Dynamic Host Configuration Protocol	
DNS	Domain Name System	
IGMP	Internet Group Management Protocol	
ICMP	Internet Control Message Protocol	
LLDP	Link Local Discovery Protocol	Used for network monitoring and supervision.
mDNS	Multicast DNS	
OCA	Open Control Architecture	
OCP	Object Control Protocol	Used during the firmware upgrade.
PTP	Precision Time Protocol	Used for audio sample synchronization.
SAP	Session Announcement Protocol	
(R)STP	(Rapid) Spanning Tree Protocol	
TFTP	Trivial File Transfer Protocol	Used for the firmware upgrade.

3.1.2 Port usage

Communication type (Description)	Type (address)	Transport	Start port End port Listen port	Comment
Conmon (Audinate Multicast Control and Monitoring)	Multicast (224.0.0.230 - 233)	UDP	8700 8708 Yes	Available only when: – The control security is disabled. – The control security is enabled and the Dante

Communication type (Description)	Type (address)	Transport	Start port End port Listen port	Comment
				compatibility mode is activated.
Dante audio (ATP Multicast Audio)	Multicast (239.255.0.0/16)	UDP	4321 Yes	A range of 1024 addresses can be selected in the configuration interface.
mDNS/DNS-SD (Multicast DNS and DNS-based Service Discovery)	Multicast (224.0.0.251)	UDP	5353 Yes	
OCA OCP.1 (Open Control Architecture OCP.1 - Audio Control Protocol)	Unicast	TCP/UDP	49152 65535 No	The actual port is announced through SRV DNS-SD. The port is only open if the device is not running in secure mode.
OCA OCP.1 Secure (Open Control Architecture OCP.1 Secure - Secure Audio Control Protocol)	Unicast	TCP/UDP	49152 65535 No	The actual port is announced through SRV DNS-SD. The port is only open if the device implements secure OCA.
OCP (Object Control Protocol)	Unicast	TCP	9470 Yes	Used for the firmware upgrade when the CAP6 host processor is in bootloader mode.
PTPv1 (Dante clock synchronization)	Multicast (224.0.1.129-13 2)	UDP	319 320 Yes	
PTPv2 (AES67 clock synchronization)	Multicast (224.0.1.129)	UDP	319 320 Yes	
Secure OCP (Secure Object Control Protocol)	Unicast	TCP	9471 Yes	Used for the firmware upgrade when the CAP6 host processor is in bootloader mode and secure OCP is used.

3.2 CAP6

The CAP6 is subcomponent of PRAESENSA audio devices with more than two audio channels.

3.2.1 Supported protocols

Protocol	Description	Comment
AES67	AES67 audio	
ARP	Address Resolution Protocol	
Dante	Dante audio support	
DHCP	Dynamic Host Configuration Protocol	
DNS	Domain Name System	
IGMP	Internet Group Management Protocol	
ICMP	Internet Control Message Protocol	
LLDP	Link Local Discovery Protocol	Used for network monitoring and supervision.
mDNS	Multicast DNS	
OCA	Open Control Architecture	
OCP	Object Control Protocol	Used during the firmware upgrade.
PTP	Precision Time Protocol	Used for audio sample synchronization.
SAP	Session Announcement Protocol	
(R)STP	(Rapid) Spanning Tree Protocol	
TFTP	Trivial File Transfer Protocol	Used for the firmware upgrade.

3.2.2 Port usage

Communication type (Description)	Type (address)	Transport	Start port End port Listen port	Comment
AES67 (Multicast audio)	Multicast (239.x.0.0/16)	UDP	5004 Yes	The user can configure the 'x' through the Dante Control. The standard is set to 239.69.0.0/16.
Conmon (Audinate Multicast Control and Monitoring)	Multicast (224.0.0.230 - 233)	UDP	8700 8708 Yes	Available only when: – The control security is disabled. – The control security is enabled and the

Communication type (Description)	Type (address)	Transport	Start port End port Listen port	Comment
				Dante compatibility mode is activated.
Dante (Dante Unicast Audio)	Unicast	UDP	14336 14591 	The actual port is negotiated during the audio setup.
Dante audio (ATP Multicast Audio)	Multicast (239.255.0.0/16)	UDP	4321 Yes	A range of 1024 addresses can be selected in the configuration interface.
mDNS/DNS-SD (Multicast DNS and DNS-based Service Discovery)	Multicast (224.0.0.251)	UDP	5353 Yes	
OCA OCP.1 (Open Control Architecture OCP.1 - Audio Control Protocol)	Unicast	TCP/UDP	49152 65535 No	The actual port is announced through SRV DNS-SD. The port is only open if the device is not running in secure mode.
OCA OCP.1 Secure (Open Control Architecture OCP.1 Secure - Secure Audio Control Protocol)	Unicast	TCP/UDP	49152 65535 No	The actual port is announced through SRV DNS-SD. The port is only open if the device implements secure OCA.
OCP (Object Control Protocol)	Unicast	TCP	9470 Yes	Used for the firmware upgrade when the CAP6 host processor is in bootloader mode.
PTPv1 (Dante clock synchronization)	Multicast (224.0.1.129-132)	UDP	319 320 Yes	
PTPv2 (AES67 clock synchronization)	Multicast (224.0.1.129)	UDP	319 320 Yes	

Communication type (Description)	Type (address)	Transport	Start port End port Listen port	Comment
Secure OCP (Secure Object Control Protocol)	Unicast	TCP	9471 Yes	Used for the firmware upgrade when the CAP6 host processor is in bootloader mode and secure OCP is used.

3.3 System controller

The system controller has two Ethernet connections:

– One for the audio device part
– One for the controller part

The CAP6 subcomponent is found in the audio device part of the system controller.

3.3.1 Device part - Supported protocols

Protocol	Description	Comment
CAP6 protocols	Refer to *Supported protocols, page 15*	

3.3.2 Device part - Port usage

Communication type (Description)	Type	Transport	Start port Listen port	Comment
CAP6 ports (Refer to *Port usage, page 15*)				The CAP6 ports are applicable only in secure mode and with the Dante compatibility disabled.
OCA (Open Control Architecture OCP.1 - Audio Control Protocol)	Unicast	TCP	49152 Yes	

3.3.3 Controller part - Supported protocols

Protocol	Description	Comment
	PRAESENSA Open Interface	Used to connect with third-party devices and the Logging applications.
ARP	Address Resolution Protocol	
CARP	Common Address Redundancy Protocol	Used for redundant system controllers. The user can select the Virtual Host ID in the configuration interface.

Protocol	Description	Comment
Dante	Dante audio support	
DHCP	Dynamic Host Configuration Protocol	
DNS	Domain Name System	
HTTP(S)	Hypertext Transfer Protocol (Secure)	
ICMP	Internet Control Message Protocol	
mDNS	Multicast DNS	
NTP	Network Time Protocol	
OCA	Open Control Architecture	
RTP	Real-time Transport Protocol	Used for VoIP audio transport.
SAP	Session Announcement Protocol	
SIP	Session Initiation Protocol	Used for VoIP support.
SNMP	Simple Network Management Protocol	Used for the supervision of supported switches.
SSH	Secure Shell	
TFTP	Trivial File Transfer Protocol	Used for the firmware upgrade.

3.3.4 Controller part - Port usage

Communication type (Description)	Type (address)	Transport	Start port End port Listen port	Comment
Ephemeral port range (for various communication purposes)		TCP/UDP	32768 60999 No	
CARP (Common Address Resolution Protocol)	Multicast (224.0.0.18)			
Conmon (Audinate Multicast Control and Monitoring)	Multicast (224.0.0.230 - 233)	UDP	8700 8708 Yes	
Conmon (Audinate Multicast Control and Monitoring)	Unicast	UDP	8800 Yes	Audinate internal port. Refer to the Audinate FAQ for details.
Dante control (Audio control)	Unicast	UDP	4440 	

Communication type (Description)	Type (address)	Transport	Start port End port Listen port	Comment
			Yes	
Dante control (Audio control)	Unicast	UDP	4455 Yes	
DNS-SD helper (Domain Name System-based Service Discovery Helper)	Unicast	UDP	9474 Yes	
DNS-SD Reconfirm Relay (Domain Name System-based Service Discovery Reconfirm Relay port)	Unicast	UDP	9475 Yes	
HTTP (Hypertext Transfer Protocol)	Unicast	TCP	80 Yes	Used for the configuration interface. Redirects to the HTTPS port.
HTTPS (Hypertext Transfer Protocol Secure)	Unicast	TCP	443 Yes	Used for the configuration interface.
IEC 61162-450 BAM (BAM transmission groups)	Multicast (239.192.0.17-18)	UDP	60017 60018 No	Used when the PRA-LSMED is enabled in the system controller.
IEC 61162-450 CAM (CAM transmission groups)	Multicast (239.192.0.19-20)	UDP	60019 60020 Yes	Used when the PRA-LSMED is enabled in the system controller.
IEC 61162-450 SRP (System Function ID resolution)	Multicast (239.192.0.56)	UDP	60065 Yes	Used when the PRA-LSMED is enabled in the system controller.
mDNS/DNS-SD (Multicast DNS and DNS-based Service Discovery)	Multicast (224.0.0.1)	UDP	5350 Yes	Socket used for Network Address Translation Port Mapping Protocol (NAT-PMP).
mDNS/DNS-SD	Multicast (224.0.0.251)	UDP	5353 	

Communication type (Description)	Type (address)	Transport	Start port End port Listen port	Comment
(Multicast DNS and DNS-based Service Discovery)			Yes	
NTP (Network Time Protocol)	Unicast	UDP	123 Yes	Used for time synchronization.
OCA OCP.1 (Open Control Architecture OCP.1 - Audio Control Protocol)	Unicast	TCP	65000 Yes	Used for VoIP communication.
OCA OCP.1 Secure (Open Control Architecture OCP.1 Secure - Secure Audio Control Protocol)	Unicast	TCP	61001 Yes	Used for the call station device.
OCA OCP.1 Secure (Open Control Architecture OCP.1 Secure - Secure Audio Control Protocol)	Unicast	TCP	65000 Yes	Used for VoIP communication.
Open Interface	Unicast	TCP	9401 Yes	Non-secure Open Interface client.
Open Interface Secure	Unicast	TCP	9403 Yes	
SAP (AES67 multicast streams discovery)	Multicast (239.255.255.255)	UDP	9875 Yes	Available only when AES67 is enabled.
SIP (Session Initiation Protocol)	Unicast	UDP	5060 Yes	Used for VoIP audio.
SIP RTP/RTCP (Session Initiation Protocol Real-Time Transport/Real-Time Control Protocol)	Unicast	UDP	10000 20000 No	Used for VoIP audio. It is bidirectional.

Communication type (Description)	Type (address)	Transport	Start port End port Listen port	Comment
SIP Secure (Session Initiation Protocol Secure)	Unicast	TCP	5061 No	Used for VoIP audio with signaling through TLS.
SSH (Secure Shell)	Unicast	TCP	22 Yes	Only used for the synchronization between redundant controllers.

3.4 Call station

The CAP2 subcomponent is found in the call station.
The call station has two Ethernet connections:
- One for the application processor
- One for the GUI processor

3.4.1 Supported protocols

Protocol	Description	Comment
CAP2 protocols	Refer to *Supported protocols, page 15*	AES67 is not enabled.
HTTP	Hyper Text Transfer Protocol	Used to download OSS licenses.

3.4.2 Port usage

Communication type (Description)	Type	Transport	Start port End port Listen port	Comment
CAP2 ports (Refer to *Port usage, page 15*)				The CAP2 ports are applicable only in secure mode and with the Dante compatibility disabled.
HTTP (Hypertext Transfer Protocol)	Unicast	TCP	80 Yes	Used to download OSS licenses. Applicable only to the GUI processor.
OCA (Open Control Architecture OCP.1 - Audio Control Protocol)	Unicast	TCP	49152 Yes	Applicable only to the Application processor.
OCA OCP.1 Secure	Unicast	TCP/UDP	49152 65535 No	Applicable only to the GUI processor.

Communication type (Description)	Type	Transport	Start port End port Listen port	Comment
(Open Control Architecture OCP.1 Secure - Secure Audio Control Protocol)				

3.5 Amplifier

The CAP6 subcomponent is found in the amplifier.

3.5.1 Supported protocols

Protocol	Description	Comment
CAP6 protocols	Refer to *Supported protocols, page 15*	AES67 is not enabled.

3.5.2 Port usage

Communication type (Description)	Type	Transport	Start port Listen port	Comment
CAP6 ports (Refer to *Port usage, page 15*)				The CAP6 ports are applicable only in secure mode and with the Dante compatibility disabled.
OCA (Open Control Architecture OCP.1 - Audio Control Protocol)	Unicast	TCP	49152 Yes	

3.6 Multifunction power supply / Audio interface module

The CAP2 subcomponent is found in the multifunction power supply and in the audio interface module.

3.6.1 Supported protocols

Protocol	Description	Comment
CAP2 protocols	Refer to *Supported protocols, page 15*	AES67 is not enabled.

3.6.2 Port usage

Communication type (Description)	Type	Transport	Start port / Listen port	Comment
CAP2 ports (Refer to *Port usage, page 15*)				The CAP2 ports are applicable only in secure mode and with the Dante compatibility disabled.
OCA (Open Control Architecture OCP.1 - Audio Control Protocol)	Unicast	TCP	49152 / Yes	

3.7 Ambient noise sensor / Control interface module / Wall control panel

3.7.1 Supported protocols

Protocol	Description	Comment
ARP	Address Resolution Protocol	
DHCP	Dynamic Host Configuration Protocol	
DNS	Domain Name System	
ICMP	Internet Control Message Protocol	
LLDP	Link Local Discovery Protocol	Used for network monitoring and supervision.
mDNS	Multicast DNS	
OCA	Open Control Architecture	
OCP	Object Control Protocol	Used during the firmware upgrade.
(R)STP	(Rapid) Spanning Tree Protocol	
TFTP	Trivial File Transfer Protocol	Used for the firmware upgrade.

3.7.2 Port usage

Communication type (Description)	Type (address)	Transport	Start port / Listen port	Comment
mDNS/DNS-SD (Multicast Domain Name System and Domain Name System-based Service Discovery)	Multicast (224.0.0.251)	UDP	5353 / Yes	
OCA	Unicast	TCP	49152	

Communication type (Description)	Type (address)	Transport	Start port Listen port	Comment
(Open Control Architecture OCP.1 - Audio Control Protocol)			Yes	
OCP (Object Control Protocol)	Unicast	TCP	9470 Yes	Used for firmware upgrade.
Secure OCP (Secure Object Control Protocol)	Unicast	TCP	9471 Yes	Used for firmware upgrade.

3.8 Ethernet switch

3.8.1 Supported protocols

Protocol	Description	Comment
ARP	Address Resolution Protocol	
DHCP	Dynamic Host Configuration Protocol	
DNS	Domain Name System	
HTTPS	Hypertext Transfer Protocol	
ICMP	Internet Control Message Protocol	
IGMP	Internet Group Management Protocol	
NTP	Network Time Protocol	
SNMP	Simple Network Management Protocol	Used for the supervision of supported switches.
(R)STP	Rapid Spanning Tree Protocol	
TFTP	Trivial File Transfer Protocol	Used for the firmware upgrade.

3.8.2 Port usage

Communication type (Description)	Type (address)	Transport	Start port Listen port	Comment
HTTPS (Webserver for configuration	Unicast	TCP	443	
SNMP (Used for supervision)	Unicast	TCP	161	

3.9 Logging applications

The Logging applications are Windows PC-based tools for collecting and viewing events from the PRAESENSA controller.

3.9.1 Supported protocols

Protocol	Description	Comment
	PRAESENSA Open Interface	User to connect with third-party devices.
.Net WCF	Logging viewer-server communication	

3.9.2 Port usage

Communication type (Description)	Type (address)	Transport	Start port Listen port	Comment
Open Interface secure (Open Interface secure to system controller	Unicast	TCP	9403	
Microsoft remoting (Interface between the Logging Viewer and the Logging Server)	Unicast	TCP	19451 Yes	Listen port on the Logging Server.

4 Security functionality verification

4.1 System controller configuration

Confirm in the configuration interface that:

1. An auto generated or a sufficiently strong Pre-Shared Key (PSK) is configured for the communication between the PRAESENSA devices. Refer to the section *Password policy* in the *System settings* chapter of the configuration manual.
2. The right credentials are setup for the following types of users and that they can be used to gain access to the system:
   - Administrator
   - Installer
   - Operator
   - Refer to the *User accounts* chapter in the configuration manual.
3. The system clients are configured for the expected Open Interface system clients.
4. Access by non-configured system clients is disabled. Refer to the section *Allow access by non-configured system clients* in the *System settings* chapter of the configuration manual.
5. The emergency control from the Open Interface is disabled.
6. The session timeouts are correctly configured for the configuration interface. Refer to the section *Automatic logout after inactivity of* in the *System settings* chapter of the configuration manual.
7. The emergency call stations have physical protection or are installed in a restricted area fitting to the purpose of the user interface.
8. Non-emergency call stations:
   - Are configured for priorities below the emergency range. Refer to the *Call definitions* chapter in the configuration manual.
   - Have authentication enabled for locations that can have public access.
   - Have the correct users assigned.
   - Have the correct session timeout configured.
   - For call station authentication, refer to the *Access control users* chapter and to the *Call station* chapter in *Device options*, both in the configuration manual.
9. Dante inputs are only configured for background and business purposes, and, as such, do not have an emergency priority assigned. Refer to the *System controller* chapter in *Device options* in the configuration manual.
10. Voice over IP (VoIP) is:
    - Not configured.
    - Or, when configured, that VoIP calls are only for business purposes, and, as such, do not have an emergency priority assigned.
11. Only secure communication with the SIP server is used.
12. It is possible to back up the PRAESENSA configuration including the messages. Refer to the *Back and restore* chapter in the configuration manual.
13. The backup can be restored. Make the backup available on-board for recovery purposes.

4.2 Logging applications

1. Confirm in the configuration interface that the authentication is enabled for the Logging Server. Refer to the *Optional: Use the Logging Server* chapter in the configuration manual.
2. Confirm in the configuration interface that the system controller authentication that is used for the connection between the Logging Server and the system controllers is based on an Operator account.
3. Confirm that the Logging Server and Logging Viewer are installed on the same machine.

4. Confirm that the computer running the Logging Server and the Logging Viewer is physically protected.
5. Confirm that the users of the computer that runs the Logging applications are required to log in to use the Logging Server and the Logging Viewer.
6. Confirm that the event log is accessible in the Logging Viewer.
7. Confirm that the new events from the system controller appear in the Logging Viewer.

4.3 Ethernet switch

1. Confirm in the configuration interface that only the necessary users have the defined credentials. Refer to the chapter *Network switch* within *Device options* in the configuration manual.
2. Confirm in the configuration interface and in the configuration settings of the switch that the correct password policy is defined.
3. Confirm that the passwords comply with the policy.

4.4 Installation

1. Confirm in the configuration interface, or by analyzing the network traffic, that the Open interface clients only use the secure port to connect to the system controller.
2. Confirm that the used IP-addresses, address ranges, and Netmasks, comply to the on-board network specifications.
3. Confirm that PRAESENSA is installed with a redundant power supply.
4. Confirm that a firewall is installed between PRAESENSA and any untrusted network.
5. Confirm that the firewall performs as expected through a port scan from both sides.
6. In case the normal operation of the PRAESENSA system can no longer be maintained, confirm that the behavior of the devices connected to PRAESENSA is as expected. The PRAESENSA behavior in such case is defined as:
   - Devices that disconnect from the system controller due to communication disruption stop distributing audio. The output contacts are deactivated, with the exception of the output contacts that are used in an emergency call, or that are configured to be fault output contacts that are activated to indicate a fault. The user interface of the device shows disconnected and fault state.
   - Restarted devices enter the startup state until the connection with the system controller is reestablished. The audio distribution by the device is stopped. The user interface of the device shows disconnected and fault state.
   - The amplifiers that have no connection with the system controller, or experience a total failure of the control board, switch to lifeline mode. In lifeline mode, an analog signal is fed to the amplifier stages. The lifeline signal is received from the multifunction power supplies to which the system routes the highest priority emergency call for lifeline purposes.
7. Confirm that the PRAESENSA devices are installed in a restricted area in lockable racks.
8. Confirm that the cabling is protected.
9. Confirm that the Ethernet ports are covered for devices that are in a non-protected area.

4.5 Firewall configuration rules

Follow these rules to access the PRAESENSA system controller from an untrusted network for connection to the Open Interface or Voice over IP (VoIP).

Open interface

Follow these rules if you need to connect to the Open Interface from an untrusted network.

#	Protocol	Source	Source port	Destination	Destination port	Action	Description
1	IPv4 TCP	Source network or source IP address	Any	System controller IP address	9403	Allow	Open Interface secure port
2	Any	Any		Any	Deny	Deny	Catch-all

VoIP

Follow these rules if you need the telephone feature from an untrusted network.

#	Protocol	Source	Source port	Destination	Destination port	Action	Description
1	IPv4 UDP	Source network	Any	System controller IP address	10,000 ... 20,000	Allow	RTP
2	Any	Any		Any	Deny	Deny	Catch-all

5 Configuration guidelines

Find a description of the typical configuration of the PRAESENSA system in the PRAESENSA configuration manual.

The next chapters describe how to configure specific settings in the context of the IACS UR E27 standard.

5.1 Open interface protocol

If you use the open interface protocol, be aware that:

- You can only use secure connections. Only the secure port 9403 is permitted, which allows communication only through TLS. In the *System settings* page of the configuration, the user can select between **TLS1.2** and **TLS1.3**. This device configuration is based on an IP-address, allowing access to be limited to devices from other subnets. Make sure to use only explicitly configured devices for the open interface.
- A firewall is required to use the open interface with networks beyond that of the PRAESENSA system. The firewall needs to be an external device that separates and isolates the PRAESENSA network from other networks. The firewall must only allow the intended network traffic to pass through.
- The passwords used must have the following:
  - A minimum of 12 characters of length.
  - At least one uppercase character.
  - At least one number.
  - At least one special character.
- The emergency functionality accessibility of the Open Interface must be disabled in the configuration, in the *System settings* page, in the section *Open Interface*. For details, Refer to the PRAESENSA configuration manual.

The process capacity for the Open Interface protocol is as follows:

- Receiving messages: one message per second on average with a burst of 10.
- Transmitting messages:
  - One response per command
  - A burst of up to 2000 events for each event registration
  - One or more call state updates per call
  - One or more zone state updates per call.

5.2 Passwords usage

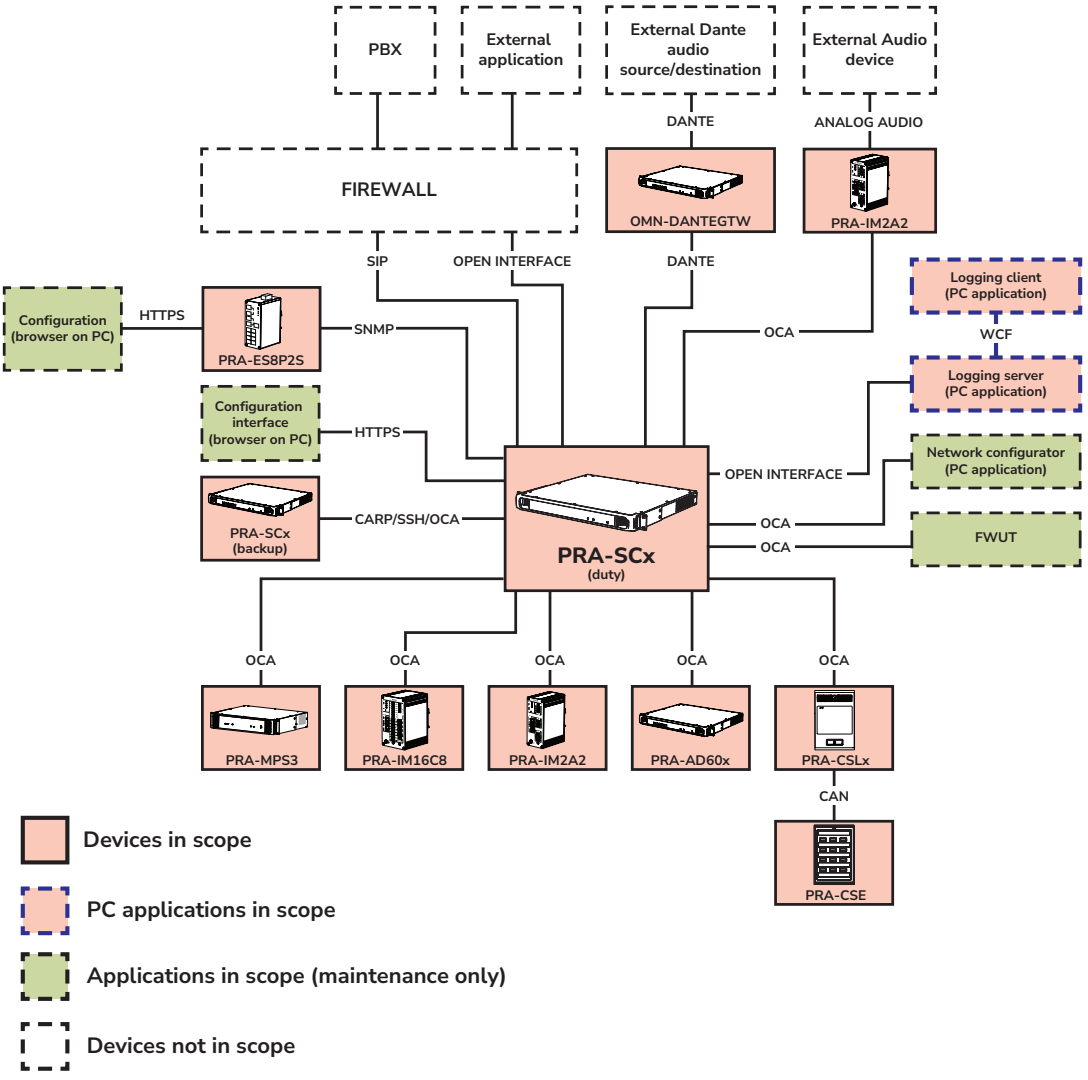
In regards to passwords, you are advised to:

- Disable the password storage in your browser.
- Use SHA as the hashing algorithm for SNMP when configuring the Ethernet switches in the system controller.

6 System topologies

The next chapters present reference topology images of the PRAESENSA system. They are examples of the many possible potential network topologies. A protocol and port overview can be found under *Communication protocols and ports, page 15*.

6.1 Logical topology

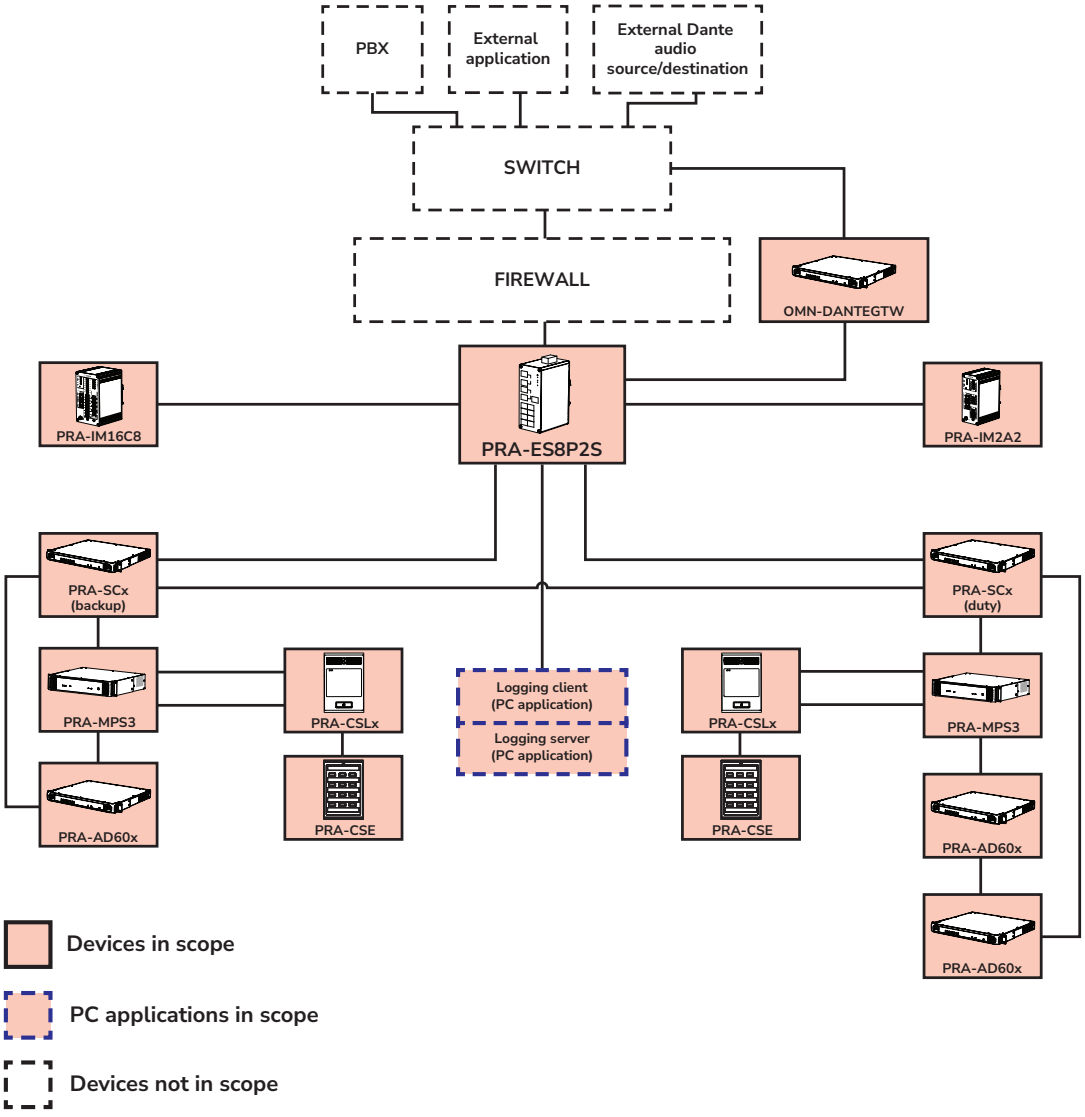


6.2 Physical topology

The physical topology below gives an example of a physical network deployment of the PRAESENSA system. Depending on the size of the system, many different deployments are possible.
The overview only shows some of the typical redundant network connections. To accommodate the required network ports, you might need more switches. The transceivers for fiber connections are omitted, but can be used for long-distance connections between distributed components.
External network devices are out of scope for PRAESENSA but might be required to achieve the intended network compartmentalization and security. Such external network devices can be:

- Switches
- Routers
- Firewalls
- Remote networks
- Intrusion detection systems.

Dante audio is transferred between networks through the OMNEO to Dante gateway, which separates the networks and only passes the audio through.



7 Incident response plan

For general safety and security information, refer to the *Security precautions*.

7.1 Forensics by use of audit records

Inspect the security audit logs:

- When a breach is suspected.
- On a regular basis, in order to detect attempts to gain unauthorized access.

Use the Logging applications to see the audit records. Refer to the following chapters in the PRAESENSA configuration manual:

- Install the system software -> Optional: Logging Server
- Install the system software -> Optional: Logging Viewer
- Optional: Using the Logging Server
- Optional: Using the Logging Viewer

7.2 Controlled shutdown, reset, roll-back and restart

You might need to restore the configuration in case of a cyberattack.
You might need to restore the duty controller in case of a redundant controller setup. The backup controllers synchronize automatically.
Visit the **Save configuration** and **Backup and restore** pages in the PRAESENSA configuration interface to roll-back and restart the system. A previously created configuration can be restored to bring the system to a previous known state. Refer to the chapters with the same names in the configuration manual for more information.

1. Disconnect the system from any untrusted networks.
2. For all system controllers PRA-SCL / PRA-SCS, press the reset to default button at the back for over 10 seconds.
3. In the configuration interface, restore a previously backed-up configuration.
4. For all Ethernet switches PRA-ES8P2S, press the default button at the back for over five seconds.
5. In the configuration interface, restore a previously backed-up configuration.
6. If necessary, power off and restart all devices.

8 Other supporting documentation

All documentation available for the PRAESENSA system can be found in the Downloads sections of the PRAESENSA devices in the catalog at https://commerce.keenfinity.tech/gb/en/Digital-PA-and-Emergency-Sound/c/3863688587. The documentation includes, among others:

Document	Description
Security precautions (SSI)	Describes the hardening guidelines of the system. Available as a single document and part of the IM, CM, and others.
Datasheets	Presents a specific hardware device or software license. Includes technical data.
Installation manual (IM)	Describes the installation procedure of all hardware devices.
Configuration manual (CM)	Describes the configuration of the system and supporting software applications.
Release notes (RLN)	Describes the new functionalities and fixes of all released versions.
Quick installation guides (QIG)	Describes the installation procedure of one or, if similar, multiple hardware devices. The QIGs accompany the product
Architect and Engineering Specifications (AE)	Describes the functionalities of the hardware devices and software licenses. Available as a single document and part of the datasheets and IM.

9 Checklist

This list summarizes the mandatory settings for an UR E27-approved PRAESENSA system. All items must be fulfilled.
For further details on the topics, check the referred chapters.

Item		Y / N
Refer to *System controller configuration*, *page 28*.		
1	An auto generated or a sufficiently strong Pre-Shared Key (PSK) is configured for the communication between the PRAESENSA devices.	
2	The right credentials are setup for respective types of users.	
3	The credentials can be used to gain access to the system.	
4	The system clients are configured for the expected Open Interface system clients.	
5	Access by non-configured system clients is disabled.	
6	The emergency control from the Open Interface is disabled.	
7	The session timeouts are correctly configured for the configuration interface.	
8	The emergency call stations have physical protection or are installed in a restricted area fitting to the purpose of the user interface.	
9	Non-emergency call stations are configured for priorities below the emergency range.	
10	Non-emergency call stations have authentication enabled for locations that can have public access.	
11	Non-emergency call stations have the correct users assigned.	
12	Non-emergency call stations have the correct session timeout configured.	
13	Dante inputs are only configured for background and business purposes.	
14	Dante inputs do not have an emergency priority assigned.	
15	Voice over IP (VoIP) is not configured.	
16	If configured, VoIP calls do not have an emergency priority assigned.	
17	If configured, VoIP calls are only for business purposes.	
18	Only secure communication with the SIP server is used.	
19	It is possible to back up the PRAESENSA configuration including the messages.	
20	The PRAESENSA backup can be restored and is available on-board for recovery purposes.	
21	The PRAESENSA backup is available on-board for recovery purposes.	
22	NTP is enabled in the system controller.	
Refer to *Logging applications*, *page 28*.		
23	The authentication is enabled for the Logging Server.	

24	The system controller authentication used for the connection between the Logging Server and the system controllers is based on an Operator account.	
25	The Logging Server and Logging Viewer are installed on the same machine.	
26	The computer running the Logging Server and the Logging Viewer is physically protected.	
27	The users of the computer that runs the Logging applications are required to log in to use the Logging Server and the Logging Viewer.	
28	The event log is accessible in the Logging Viewer.	
29	New events from the system controller appear in the Logging Viewer.	
Refer to *Ethernet switch, page 29* and *Safety and security information, page 5*.		
30	The default user is removed.	
31	The initial password is changed.	
32	Only the necessary users have the defined credentials for the Ethernet switch.	
33	The SNMP credentials configured in the switch match the credentials of the system controller.	
34	The correct password policy is defined in PRAESENSA and in the Ethernet switch.	
35	The passwords comply with the correct password policy.	
36	Encrypted SNMPv3 communication with enabled SHA authentication protocol and AES privacy protocol are used for read-only access.	
37	NTP is enabled in the switch.	
38	The switch is configured to log into file storage, not into buffer.	
39	62443 Security is enabled.	
40	Signed Firmware Upgrade is enabled.	
Refer to *Installation, page 29*.		
41	The Open interface clients only use the secure port to connect to the system controller.	
42	The used IP-addresses, address ranges, and Netmasks, comply to the on-board network specifications	
43	The PRAESENSA system is installed with a redundant power supply.	
44	A firewall is installed between the PRAESENSA system and any untrusted network.	
45	The firewall performs as expected.	
46	If the normal operation of the PRAESENSA system can no longer be maintained, the behavior of the devices connected to PRAESENSA is as expected	
47	The PRAESENSA devices are installed in a restricted area in lockable racks.	
48	The cabling is protected.	

49	The Ethernet ports are covered for devices that are in a non-protected area.	
Refer to *Firewall configuration rules, page 29*.		
50	If connected to the Open Interface from an untrusted network, the rules described in *Firewall configuration rules, page 29* are followed.	
51	If connecting through the telephone interface from an untrusted network, the rules described in *Firewall configuration rules, page 29* are followed.	

Refer to

– *OMNEO to Dante gateway, page 13*

Electro Voice Dynacord B.V.
Achtseweg Zuid 173
5651 GW Eindhoven
The Netherlands
www.keenfinity-group.com

202606300844