STORZ

KARL STORZ — ENDOSKOPE

en

System Security Plan
KARL STORZ OR1 FUSION, Rel. 1.4.2

WO300

11-2020

Inhaltsverzeichnis

1 Foreword

This document is supplied by KARL STORZ SE & Co. KG (KARL STORZ) in order to provide the operator with information to be used for the integration of KARL STORZ OR1 FUSION® into the operator's IT-network. This document was generated based on KARL STORZ current knowledge of IT-networks and is subject to change as conditions in this area change/advance. Since framework conditions, installations, and the operation of the network are the responsibility of the operator, KARL STORZ cannot fully guarantee failure-free operation. The operator must ensure the protection, safety, and reliability of the IT-network through the operator's own risk management procedures in accordance with IEC 80001-1 and any additional guidelines, laws and regulations that are relevant.

2 Information

2.1 Information of the System

This System Security Plan provides an overview of the security requirements KARL STORZ OR1 FUSION and describes the controls in place or planned for implementation to provide a level of security appropriate for the information to be transmitted, processed or stored by the system. Proper management of information technology systems is essential to ensure the confidentiality, integrity and availability of the data transmitted, processed or stored by the KARL STORZ OR1 FUSION information system.

The security safeguards implemented for the KARL STORZ OR1 FUSION system meet the policy and control requirements set forth in this System Security Plan. All systems are subject to monitoring consistent with applicable laws, regulations, agency policies, procedures and practices.

Unique Identifier	Information System Name	Information System Abbreviation	Software Version	Software Version Date
WO300	KARL STORZ OR1 FUSION CONTROL	KARL STORZ OR1 FUSION	1.4.2	16.04.2020

Tab. 1: Information System Name and Title

2.2 Information System Categorization

The overall information system Cybersecurity Device Characterization Level is recorded in Table Cybersecurity Device Characterization Level that follows.

Cybersecurity Device Characterization Level :	Moderate (M)

Tab. 2: Cybersecurity Device Characterization Level

ℹ The Cybersecurity Device Characterization Level *Moderate* utilizes technical controls from the NIST 800-53 control set for Moderate Impact Systems.

2.3 Assignment of Security Responsibility

The KARL STORZ Security Owner is responsible for ensuring that the correct security control compliment and build configuration is applied at product design and to then monitor the system for security updates and review security patch releases post product release.

In Germany, you can contact the System Owner through Repair and Service Department:

KARL STORZ SE & Co.KG
Repair Service Department
Take-off Gewerbepark 83
78579 NEUHAUSEN, Germany

Service Hotline: +49 (0)7461 708-980
E-mail: technicalsupport@karlstorz.com

In other countries, the respective KARL STORZ branches or specialist dealers are responsible.

3 General System Description

3.1 Short description of the KARL STORZ OR1 FUSION system

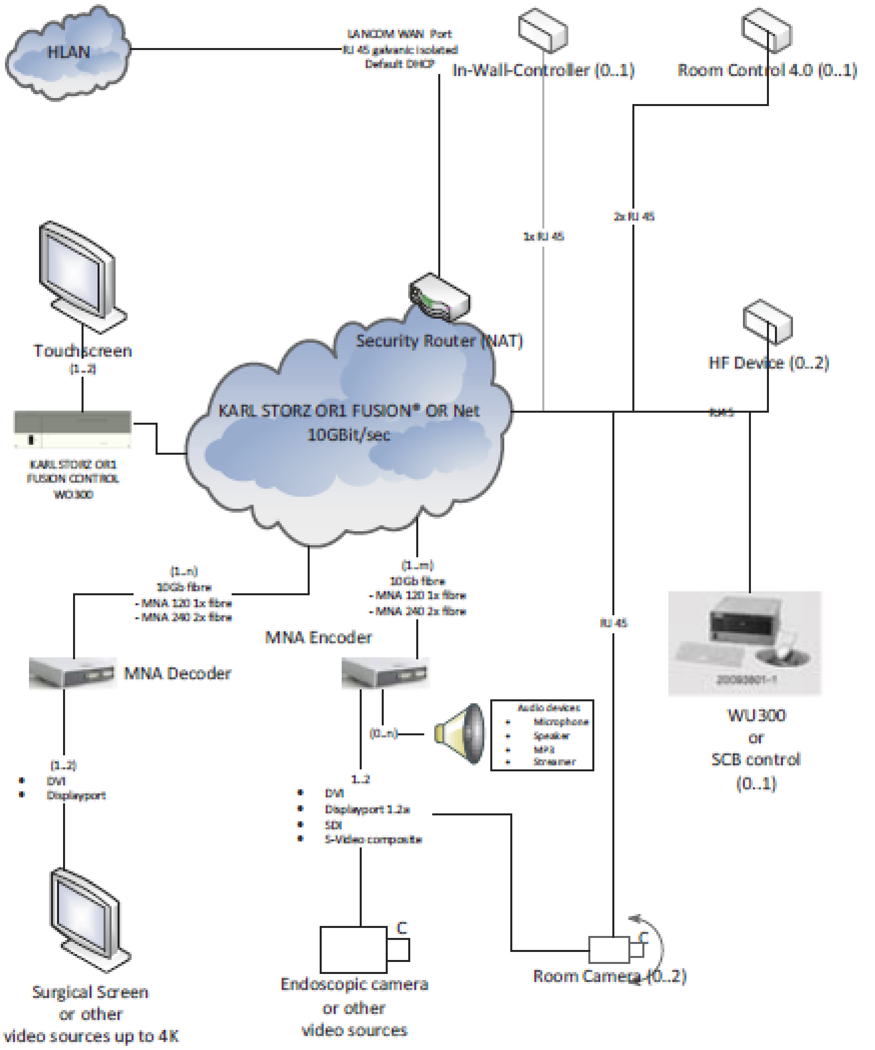
KARL STORZ OR1 FUSION® Hardware:

A dedicated assembly of devices designed to electronically receive, collect, store, manage, assist in analysis of, display, output, and distribute audiovisual data to support investigative and treatment activities in an operating room (OR). The system can be used to manage the distribution of video and audio from multiple sources to multiple peripheral devices, to control medical and non- medical devices and for documentation purposes (e.g. to store still images, video, and audio sequences during medical interventions). The system consists of dedicated combined hardware (e.g. computers, terminals, network components) and software (typically embedded).

KARL STORZ OR1 FUSION® Software:

An application software program, routines, and/or algorithms intended to be used in an operating room audiovisual information system to enable the system to function according to its intended purpose. The software typically supports remote control of medical and non-medical devices, data management/documentation and data communication/transfer within and out of the operating room (OR) [e.g., teleconferencing, teaching/ telesurgery, networking with hospital systems]. It is typically installed into a dedicated integrated network of computers and peripherals.

3.2 System Function or Purpose



The KARL STORZ OR1 FUSION® system is defined to be used in a medical environment, especially in Operating Rooms.

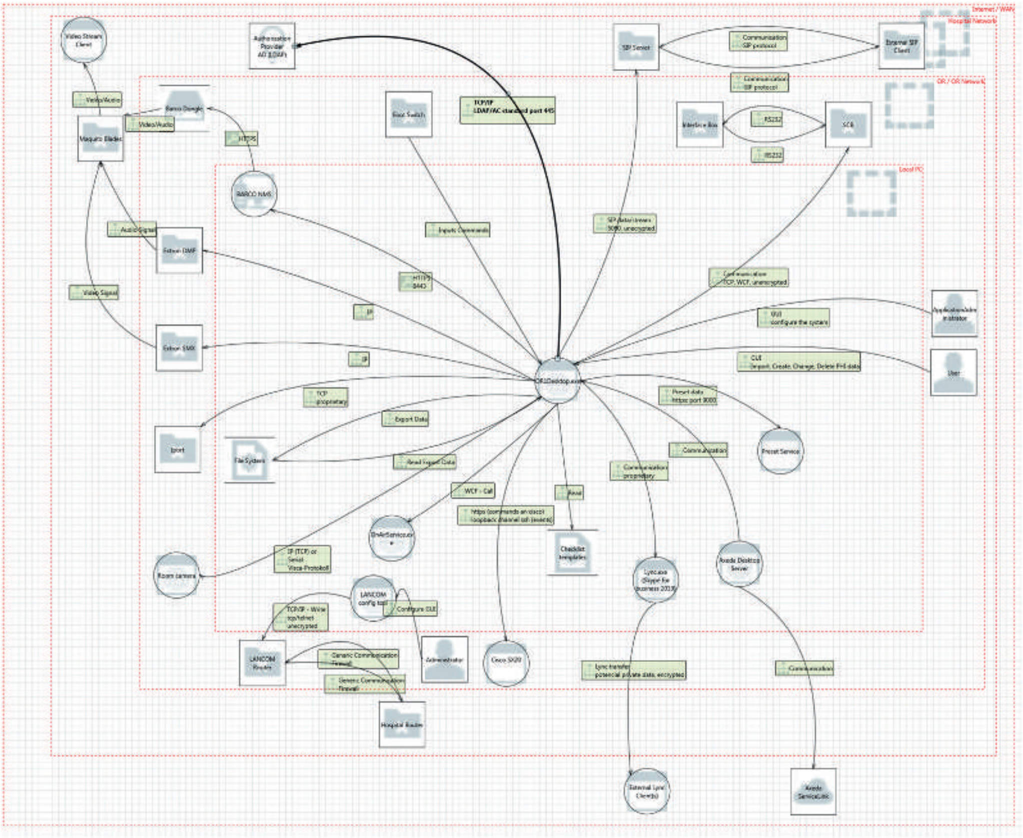
Regarding the network topology design in direction to the hospital network, the system is designed to assist in medical interventions in cases of documentation and communication.

The following general communications are supported:

- Storage of still images, streaming media, audio sequences on a Hospital File Server
- DICOM storage and Worklist
- HL7 Patient query and export of MDM/ORU messages

Reference Manufacturer Disclosure Statement for Medical Device Security for the Device Intended Use see Appendix.

3.2.1 Network Connections



The OR network is separated from the hospital network by a security router. This router blocks all connection requests from the hospital network to OR (except port 104 DICOM).

The IP range 192.168.1.0/24 and 10.179.x.0/24 is used internal. It this Range also used in the hospital, then collision are possible.

Digital Imaging and Communications in Medicine (DICOM)

For further information refer to the KARL STORZ OR1 FUSION® “DICOM Conformance Statement”.

File Transfer Protocol (FTP)

The KARL STORZ OR1 FUSION® system uses passive FTP when exporting data to a FTP server within the IT hospital network infrastructure. That means, all connections are established from the FTP client to the server.

The required FTP credentials to connect to the FTP server need to be configured and stored within the KARL STORZ OR1 FUSION®system. Used TCP-Ports 20/21.

Please refer to the FTP definition in RFC 959 for more detailed information.

FTP-server: e.g. vsftpd, Filezilla FTP server for saving patient data.

Network Share (Server Message Block SMB)

The KARL STORZ OR1 FUSION® system uses the SMB protocol standard when exporting data to a network share on a SMB server within the IT network infrastructure. Hereby all connections are established from the SMB client to the server. Therefor no special firewall configuration of the router is required. Hereby all connections are established from the SMB client to the server. Therefor no special firewall configuration of the router is required.

The required credentials to connect to the SMB server need to be configured and stored within the KARL STORZ OR1 FUSION® system.

New Windows® systems use primary TCP-Port 445. Older systems or other compatible Operation Systems (OS) can use different ports.

Please refer to the SMB definition by Microsoft under http://msdn.microsoft.com/en-us/library/cc246482.aspx for more detailed information.

Due to Cyber Security reasons, the SMBv1 Windows® feature is deactivated by default.

SMB-server: e.g. Windows® based server (Windows® server 2008), Samba (Version 4) for saving patient data.

HL7 communication (HL7 server / HIS)

The KARL STORZ OR1 FUSION® system uses the most common HL7 transport method to send HL7 messages, called Lower Layer Protocol (LLP). The Lower Layer Protocol sends unencrypted HL7 messages via TCP/IP over a local area network, such as those found in a hospital. When using LLP, an HL7 message must be wrapped using a header and trailer (also called a footer) to signify the beginning and end of a message.

OR1™ STREAMCONNECT®II - Server

For audio/video communication outside the OR-Environment an additional server platform is available.

For further information please refer to the country based assigned Whitepaper:

United States / Canada / Mexico: STREAMCONNECT® NEO

Rest of the world: Whitepaper OR1™ STREAMCONNECT® II System

Network Printer

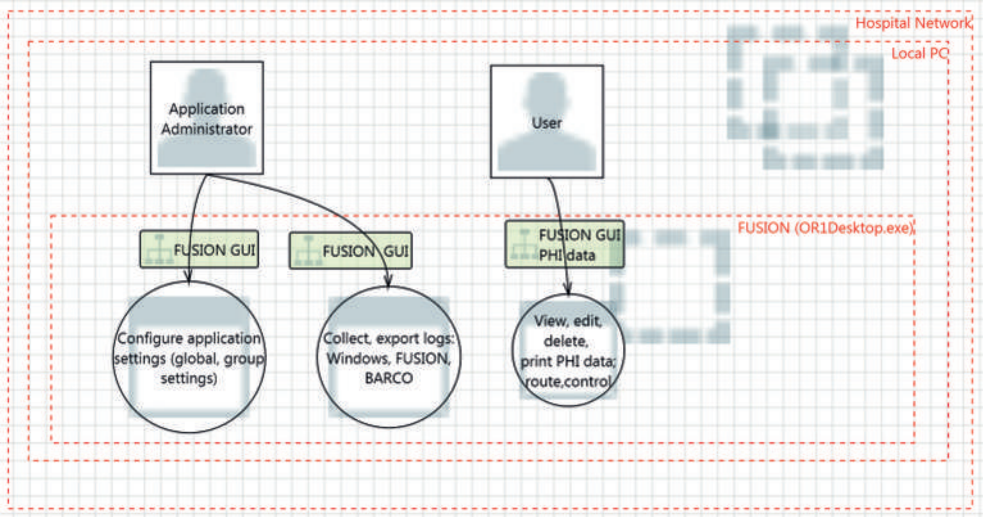
The KARL STORZ OR1 FUSION®system supports the configuration of network printers that can be used for printing treatment reports or still images. The required resources depend on the concrete network printing infrastructure and drivers that are used.

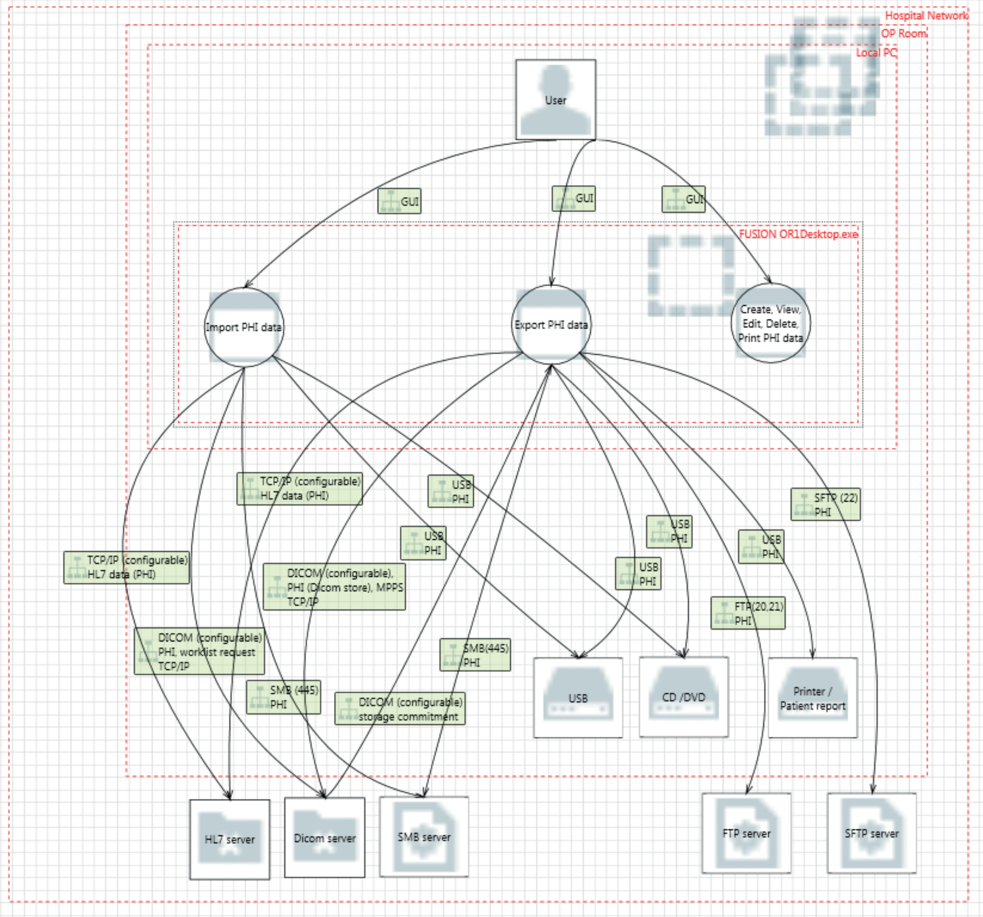
The following protocols are tested and verified:

- Network Share (Server Message Block SMB)
- Internet Printing Protocol (IPP) via TCP/UDP-Port 631
- Line Printer Daemon protocol / Line Printer Remote protocol (LPD, LPR) via TCP-Port 515
- HP-JetDirect via TCP-Port 9100

3.3 Information System Components and Boundaries

A detailed and explicit definition of the system authorization boundary diagram is represented below.


Hospital Network
Local PC
Application Administrator
User
FUSION (OR1Desktop.exe)
FUSION GUI
FUSION GUI
FUSION GUI PHI data
Configure application settings (global, group settings)
Collect, export logs: Windows, FUSION, BARCO
View, edit, delete, print PHI data; route,control


Hospital Network
OP Room
Local PC
User
GUI
GUI
GUI
FUSION OR1Desktop.exe
Import PHI data
Export PHI data
Create, View, Edit, Delete, Print PHI data
TCP/IP (configurable) HL7 data (PHI)
USB PHI
USB PHI
TCP/IP (configurable) HL7 data (PHI)
DICOM (configurable), PHI (Dicom store), MPPS TCP/IP
DICOM (configurable) PHI, worklist request TCP/IP
SMB (445) PHI
DICOM (configurable) storage commitment
SMB(445) PHI
USB PHI
USB PHI
USB PHI
SFTP (22) PHI
FTP(20,21) PHI
USB
CD /DVD
Printer / Patient report
HL7 server
Dicom server
SMB server
FTP server
SFTP server

Information Types

A list of Information Types associated with the KARL STORZ OR1 FUSION are included in Table - Sensitivity Categorization of Information Types.

Information Type	Yes/No
ePHI	Yes
ePII	Yes

Tab. 3: Table - Sensitivity Categorization of Information Types

3.4 Information System Roles

Role privileges (authorization permission after authentication takes place) are described in Table Roles and Privileges that follows.

Role	Internal or External	Privileged (P), Non-Privileged (NP), or No Logical Access (NLA)	Sensitivity Level	Authorized Privileges	Functions Performed
Application Admin	Internal	P	Severe	Custom administrative access	Configure settings applied for the local KARL STORZ OR1 FUSION® unit.incl. configure client access user access to SIP,CISCO Configuring the KARL STORZ OR1 FUSION® system for later secure usage. Download audit files.
System Administrator	Internal	P	Severe	Custom administrative access	Add system to the domain (active directory). Add, edit, and delete local user accounts and assign local users to user groups. Change network and time settings. Change autologin settings Install/configure printers. Access the Windows® desktop. Configuring the KARL STORZ OR1 FUSION® system for later secure usage. Update the system / install the patches. Configure NMS and NMA.
System Administrator	External (service)	P	Severe	Custom administrative access	Update the system / install the patches.
User	Internal	NP	Moderate	Access PII/ PHI.	Login to the KARL STORZ OR1 FUSION® system. Access patients' data in the filing cabinet. No rights to change any

Role	Internal or External	Privileged (P), Non-Privileged (NP), or No Logical Access (NLA)	Sensitivity Level	Authorized Privileges	Functions Performed
					configuration settings. Import/Export PHI data. Functional capabilities of device (e.g. Capture).

Tab. 4: Roles and Privileges

4 System Environment

The whole system consists of a combination of networking devices, non-medical devices and ME-systems according to ISO/IEC 60601-1 Part 3.64 (Definition of MEDICAL ELECTRICAL (ME) SYSTEMS): combination, as specified by its MANUFACTURER, of items of equipment, at least one of which is ME EQUIPMENT to be inter-connected by FUNCTIONAL CONNECTION or by use of a MULTIPLE SOCKETOUTLET.

As defined in Annex H of ISO/IEC 60601-1, the KARL STORZ OR1 FUSION® system is a PEMS (Programmable Electrical Medical System). The complete system is isolated from the hospital network via a software firewall. The responsibility for the network of the hospital IT administrator ends at the network port of the KARL STORZ OR1 FUSION® system. A medical system is defined in Clause 16 of ISO/IEC 60601-1. In Chapter 1 Scope of the ISO/IEC 80001 Note 4, the manufacturer who specifies a ME system that includes a network is responsible for this complete medical system. This is according to the ISO/IEC 60601-1 Part 3.64. These combinations are tested and verified as a complete system by KARL STORZ.

4.1 Requirements for network connection

The following requirements have to be fulfilled by the customer; otherwise correct function of the KARL STORZ OR1 FUSION system isn’t guaranteed:

- The availability of a gateway and DNS-Server for the KARL STORZ OR1 FUSION system should be ensured
- A minimum bandwidth of 100Mbit/s has to be guaranteed
- NTP server should be available for time synchronization in KARL STORZ OR1 FUSION and all connected systems.

KARL STORZ OR1 FUSION can read and write up to 1GBit/sec during storage operations.

4.2 Hazardous situations resulting from a failure of the IT-NETWORK

A loss of the network connection has no influence on patient safety during treatment. If the network connection is lost when treatment records are transferred to the server, the files will be retransmitted once the network connection is available again. If the network connection cannot be restored, the files created during treatment can be exported to a USB mass storage device.

Connection of the Karl Storz Medical Device to a network/data coupling that includes equipment that is not validated for use with the Karl Storz equipment could result in previously unidentified risks to patients, or operators. The operator should identify, analyse, and control such risks. This includes any subsequent changes to the network introducing new risks and requiring new analysis. Examples of pertinent changes to network include:

- changes in network configuration
- connection of additional items to network
- disconnecting items from network
- update of equipment connected to network
- upgrade of equipment connected to network

4.3 Network Ports, Protocols and Services

The ports, protocols and services enabled in this information system are listed in the following table:

Ports (TCP/UDP)*	Protocols	Services	Purpose
Configurable (Outgoing)	TCP	Dicom.Service.exe	DICOM service (support for secure transfer via SSL) – DICOM store – Worklist request DICOM MPPS
104 (Ingoing)	TCP	Dicom.Service.exe	DICOM service – Listen port to receive Storage Commitments
20/21 (Outgoing)	TCP/FTP	OR1Desktop.exe	Export of procedure files via outgoing FTP connection to export destination
22 (Outgoing)	TCP/SSH (SFTP)	OR1Desktop.exe	Export of procedure files via outgoing SSH connection to export destination
445 (Outgoing)	TCP/SMB	OR1Desktop.exe	Export of procedure files via windows share (smb) protocol
Configurable (Outgoing)	TCP	OR1Desktop.exe	HL7 query and export (DEM/ORU) messages via Lower Layer Protocol (LLP)
443 and 17002 (Outgoing)	TCP/UDP	AxedaDesktopServer.exe	Remote access to KARL STORZ OR1 FUSION® system
	TCP/UDP	Lync.exe	Skype for Business
5060 (Outgoing)	SIP	OR1Desktop.exe	SIP Telephony
22/443 (Outgoing)	TCP/SSH/HTTPS	OR1Desktop.exe	Control of Videoconference system
8443 (Only OR internal)	HTTPS	BARCO NMS	Master of Videorouting components
	UDP/multicast	BARCO direct show	Videostreams over IP
9000 (only local PC internal)	HTTPS	Preset service	Store settings from scenarios
Only OR internal	TCP/VISCA	OR1Desktop.exe	Room Camera Control
Only OR internal	TCP	LANCOM Configurator	Configuration of Router

Tab. 5: Ports, Protocols and Services

* Transmission Control Protocol (TCP), User Diagram Protocol (UDP)

5 System Interconnections

SP* IP Address and Interface	External Organization Name and IP Address of System	Connection Security (IPSec VPN, SSL, Certificates, Secure File Transfer, etc.)**	Data Direction (inbound, outbound, or both)	Information Being Transmitted	Port or Circuit Numbers
	Karlstorz.axeda.com	HTTPS	Both	Device event log Patch file	443
	Configurable	TCP/SSH/HTTPS	Both	CISCO Video-conference control	22, 443
	Configurable	TCP/UDP	Both	SIP/Lync Video-conference	40803-40842 49152-49191

Tab. 6: System Interconnections

*Service Processor
**Internet Protocol Security (IPSec), Virtual Private Network (VPN), Secure Sockets Layer (SSL)

5.1 Remote Maintenance

Remote maintenance requires network access that connects the device to the hospital network. In accordance with the data protection laws of the respective federal state, KARL STORZ explicitly ensures that external access is established only to the device in question. The individuals accessing the device are all specifically trained and instructed KARL STORZ employees who have confirmed in writing that they have undergone instruction and will apply the corresponding procedures. KARL STORZ guarantees that no patient-related information will be used for service purposes, copied, or used in any other form.

KARL STORZ will inform the operator by phone or in writing (via e-mail with confirmation request) before performing any required remote access. KARL STORZ and the operator will agree on the required modalities, the procedures, the necessary contacts, etc., in advance. These agreements will be made in writing. Two options are available for the actual external access to the device. They are described below.

5.2 Remote access via Axeda®

By default KARL STORZ offers remote maintenance through its Axeda® software for the KARL STORZ devices located in the operating room. Connection between devices in the OR and the Axeda® Connected Access™ Remote Server is established by the device using the https protocol. Further communication between the device and the Axeda® Connected Access™ Remote server uses https tunneling.

Remote service requires two outbound ports (443 and 17002) to allow the remote service agent to connect to the remote service backend (currently Axeda®). The remote service agent is installed on the KARL STORZ OR1 FUSION only and therefore only the KARL STORZ OR1 FUSION needs access to the remote service backend. The H-LAN firewall has to allow this traffic to be passed from inside the OR to outside. In addition there are a few network management tools that will be installed on the KARL STORZ OR1 FUSION to allow the network maintenance, monitoring and troubleshooting tasks via remote service. The access to the system via Axeda® needs the confirmation of the user.

Axeda® software requirements can be viewed at www.axeda.com.

6 Laws, Regulations, Standards and Guidance

6.1 Applicable Laws and Regulations

Table Laws and Regulations includes additional laws and regulations that establish specific requirements for the confidentiality, integrity, or availability of the data in the KARL STORZ OR1 FUSION®.

Title	Date
HIPAA HITECH and Omnibus Rule	1/25/2013
EU General Data Protection Regulation	5/25/2018
EU Medical Device Regulation	5/5/2017

Tab. 7: Laws and Regulations

6.2 Applicable Standards and Guidance

Table Standards and Guidance includes in this section any additional standards and guidance specific to KARL STORZ OR1 FUSION®.

Title	Date
FDA Content of Premarket Submissions for Management of Cybersecurity in Medical Devices	2/10/2014
FDA Postmarket Management of Cybersecurity in Medical Devices	12/28/2016
NIST SP 800-53 Security and Privacy Controls for Federal Information Systems and Organizations	4/1/2013
IEC/ISO 80001-1:2010 Application of risk management for IT-networks incorporating medical devices	2010-10

Tab. 8: Standards and Guidance

7 Software Installation

System is a delivery of a complete system including hardware and software (KARL STORZ OR1 FUSION® Software and Windows® 10 LTSB).

7.1 Patch Management

KARL STORZ follows the guidelines established in the FDA Postmarket Managmeent of Cybersecurity in Medical Devices. Security patches are released based on the vulnerability exploitation meeting controlled risk or uncontrolled risk analysis.

Updates for KARL STORZ OR1 FUSION® always include relevant security patches which are tested following regulatory requirements for medical devices.

7.2 Malware/ Antivirus Defense

Classic antivirus protection is only effective if the virus definition file (= blacklist) and the program engine are regularly updated. Therefore, users are only protected against threats that are known to the manufacturer. There is a general risk of a faulty update of the antivirus program negatively affecting the system, resulting in problems as severe as total system failure. Therefore, careful checks are indispensable.

The Patch Management solution of the KARL STORZ OR1 FUSION® system is based on Nexus SE46, which starts automatically together with the Windows® operating system and uses the whitelist approach. When using a whitelist, all executable files that are not listed on the whitelist are blocked from running. As a result, any intruding malware is prevented from negatively affecting the system or changing it. This includes malware such as viruses or Trojans even if they are hidden in other files.

Only a KARL STORZ service technician has the privileges to switch the Nexus SE46 into the Service Mode, which allows full control and sole authorization to make fundamental modifications to the operating system and installations. This also applies to the release of new system components and updates.

The initial installation as well as the installation of updates or safety patches of anti-malware programs must be tested in advance within the respective environment.

Please note that the operator is responsible for malware protection in view of risk management in accordance with IEC 80001.

8 Security Controls

The System Administrator and Application Administrator in the hospital are responsible for configuring the KARL STORZ OR1 FUSION® System for later secure usage. Please consult /REF_001/ and /REF_002/ to manage cybersecurity settings corresponding to your requirements.

A list of NIST SP 800-53 security controls for KARL STORZ OR1 FUSION® system is provided in the following table:

ID	Controls
AC	AC-2, AC-3, AC-5, AC-6, AC-6(1), AC-6(2), AC-6(5), AC-6(9), AC-6(10), AC-7, AC-8, AC-14, AC-17, AC-17(2), AC-4, AC-12, AC-17(1), AC-17(3), AC-17(4), AC-18, AC-18(1)
AT	
AU	AU-2, AU-3, AU-4, AU-6, AU-8, AU-8(1), AU-9, AU-11, AU-12, AU-6(3), AU-9(4)
CA	
CM	CM-7, CM-7(2), CM-7(5), CM-11, CM-6, CM-8, CM-8(1), CM-8(3)
CP	CP-9, CP-10
IA	IA-3, IA-4
IR	
MA	MA-2, MA-4, MA-4(2)
MP	MP-2, MP-6, MP-7
PE	
PL	
PS	
RA	RA-3, RA-5
SA	
SC	SC-2, SC-5, SC-7, SC-7(5), SC-8, SC-8(1), SC-12, SC-13, SC-15, SC-10, SC-7(4), SC-28
SI	SI-3, SI-7, SI-10, SI-4(4), SI-7(1),SI-7(7)

Tab. 9: Selected security controls

9 Compensating Controls

Residual Risk ID	Threat / Vulnerability	Mitigation Strategy
HL7 message via TCP	Data transfer (PHI data) between server and KARL STORZ OR1 FUSION® could be intercepted by a man in the middle attack.	Customer is responsible for securing the hospital network from unauthorized access and the communication between KARL STORZ OR1 FUSION® and other systems. KARL STORZ OR1 FUSION® uses Lower Layer Protocol (LLP) which is standard for HL7 communication and not secured per default. In theory, LLP with the TLS (Transport Layer Security) or SSL (Secure Socket Layer) cryptographic protocol is a standard supported by the IHE organization. In practice, it doesn't seem to be used often. Most integration engines have yet to support this standard. To make the communication secure, the Network Administrators should connect the KARL STORZ OR1 FUSION® to trusted networks only, to ensure that it cannot be read by unauthorized users. Network Administrators could consider using VPN, SSH Tunneling to create secure encrypted point to point connection between the KARL STORZ OR1 FUSION® System and HL7 server.
DICOM stream with patient data via TCP/IP	Data transfer between server and the KARL STORZ OR1 FUSION® could be intercepted by a man in the middle attack.	Customer is responsible for securing the hospital network from unauthorized access and for securing the communication between the KARL STORZ OR1 FUSION® and other systems. Application Administrators should consider activating DICOM TLS encryption in the

Residual Risk ID	Threat / Vulnerability	Mitigation Strategy
		KARL STORZ OR1 FUSION® in case it is supported by the DICOM server vendor.
Patient treatment files via FTP	Data transfer between server and the KARL STORZ OR1 FUSION® could be intercepted by a man in the middle attack.	Customer is responsible for securing the hospital network from unauthorized access and for securing the communication between the KARL STORZ OR1 FUSION® and other systems. Application Administrators should consider using SFTP instead of FTP for exporting patient data.
View remote web site	DNS Spoofing in hospital network. Can be used for phishing sensitive username/ password information from e.g. STREAMCONNECT®	Customer is responsible for securing the hospital network from unauthorized access and for securing the communication between the KARL STORZ OR1 FUSION® and other systems. Application Administrators should only configure https endpoints to approved web apps to avoid Spoofing.
DICOM Worklist flat file data	Data transfer between server and the KARL STORZ OR1 FUSION® could be intercepted by a man in the middle attack.	Customer is responsible for securing the hospital network from unauthorized access and for securing the communication between the KARL STORZ OR1 FUSION® and other systems. Application Administrators should use secure transfer protocol to transport the flat file to the local KARL STORZ OR1 FUSION® machine.
Router config	The standard configuration contains default global password. Compromising of the password could allow access to router configuration allowing extend access to OR-Network trust boundary.	Change the default password for each router installation.
Password	The standard configuration contains default global password.	Change the default password for or1user and or1admin accounts.
SIP	Unencrypted data transfer containing private data (phone book), voice conver-	Hospital network administrator is responsible for securing hospital network from unauthorized access and for the

Residual Risk ID	Threat / Vulnerability	Mitigation Strategy
	sation over SIP could be intercepted by a man in the middle attack.	securing the communication between KARL STORZ OR1 FUSION® and other systems. Network administrator could consider to use VPN, SSH Tunneling, or network segmentation to create secure encrypted or point to point protected connection to transfer PHI data. Application administrator should consider to use only encrypted SMB or SFTP export instead of unencrypted protocols.
LYNC	Lync data transfer containing private data (phone book), voice conversation could be intercepted by a man in the middle attack.	Hospital network administrator is responsible for securing hospital network from unauthorized access and for the securing the communication between KARL STORZ OR1 FUSION® and other systems. Skype for business used Network administrator could consider to use VPN, SSH Tunneling, or network segmentation to create secure encrypted or point to point protected connection to realize SIP telephony.
LYNC2	Lync data transfer containing private data (phone book), voice conversation could send/save private data/conversation to Skype for business instance in the cloud and could potentially break the local law.	Hospital network administrator is responsible for securing hospital network from unauthorized access and for the securing the communication between KARL STORZ OR1 FUSION® and other systems. Communication with cloud services must be encrypted and secure. The use of cloud service and sending data to the cloud destination or persisting data must comply with all current laws (e.g. GDPR).
physical access		The physical access to the device should be protected.
autologin	Applications starts with autologin und user get access to worklist, filing cabinet and phone books.	Deactivate Windows-Autologin.
Autologin 2	Applications starts with autologin und user get access to old phi.	Deactivate fileling cabinet and use other access to phi.

10 Security exclusions

No exclusions exist.

11 Appendix

11.1 Manufacturer Disclosure Statement for the Device

STORZ
KARL STORZ—ENDOSKOPE

KARL STORZ SE & Co. KG
Dr.-Karl-Storz-Straße 34
78532 Tuttlingen

Postfach 230
78503 Tuttlingen
Germany

Phone: +49 7461 708-0
Fax: +49 7461 708-105
E-mail: info@karlstorz.com
www.karlstorz.com

JEB926 • EN • V1.0 • 11-2020 • SSP • CE-MDR