KARL STORZ AIDA® V1.3
Hospital Network Integration Requirements

PRODUCT INFO

OR1™

OR1 96 1.0 02/2017/PI-E
1/12

Change History

Version	Date	Changes	Reason	Editor
BA-03	30.11.2016	Removed not needed descriptions, added references	Review findings	TZ
BA-02	15.11.2016	Added chapter Remote Service	Review finding	TZ
BA-01	28.07.2016	Whole document	NEW	TZ

Table of Contents

Change History **2**
Table of Contents **3**
References **4**
Foreword **4**
1 Introduction **5**
1.1 Short description of the AIDA™ ME (medical electrical) system 5
1.2 Definition of a AIDA™ ME system regarding IEC 60601-1 and application regarding IEC 80001 5
1.3 Purpose of the AIDA™ ME system regarding the connection to the hospital network 5
2 IT Network Requirements **6**
2.1 Required characteristics and configuration of the hospital IT network 5
2.2 Intended information flow between the AIDA™ ME system and the IT hospital network infrastructure 6
2.2.1 Digital Imaging and Communications in Medicine (DICOM) 6
2.2.2 File Transfer Protocol (FTP) 6
2.2.3 Network Share (Server Message Block SMB) 6
2.2.4 HL7 communication (HL7 server / HIS) 6
2.2.5 KARL STORZ OR1™ STREAMCONNECT® server 7
2.2.6 Network Printer 7
3 Software Installation **7**
4 Licensing Model **7**
5 User Rights **8**
6 Availability **8**
7 Remote Service **8**
8 Patch Management of the Operating System (OS) **8**
9 Malware Defense **8**
10 Data Protection **9**
11 Data Backup and Recovery **9**
12 Network Load **10**
13 Network Ports and Protocols **10**
14 Conformity Assessment **10**
15 DICOM Conformance Statement **10**
16 Test Protocol **10**
17 System Schematic **11**

References

[REF_001]	PI_OR1_92_E_R.PDF (DICOM Conformance Statement) – 300000233325
[REF_002]	PI_OR1_93_E_R.PDF (HL7 Interface Description) – 300000233326
[REF_003]	19-C2.4.F001-CEP-W-KS05587.pdf (Clinical Evaluation) - 300000156020

Foreword

The intended use of the device / device family is defined in the following document:
See Clinical Evaluation /REF_003/ for reference.

This document is supplied by KARL STORZ in order to provide information to be used for the integration of AIDA™ into the operator's IT-network. This document was generated based on our 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, we 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 Introduction

1.1 Short description of the AIDA™ ME (medical electrical) system

AIDA™ is the name for a product aiming at integrating typical audio-video, documentation and checklist/ workflow requirements, features and functionalities for an OR environment into one single integrated system.

The AIDA™ system is a medical device according to MDD.

1.2 Definition of an AIDA™ ME system regarding IEC 60601-1 and application regarding IEC 80001

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) SYSTEM):

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 SOCKET-OUTLET.

As defined in Annex H of ISO/IEC 60601-1 the AIDA™ System is a PEMS (Programmable Electrical Medical System). The complete system is isolated from the hospital network via software firewall. The responsibility for the network of the hospital IT administrator ends at the network port of the AIDA™ 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.

1.3 Purpose of the AIDA™ ME system regarding the connection to the hospital network

The AIDA™ control system is defined to be used in 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 case of documentation and communication.

The following general communications are supported:

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

Modifying the appliance through electrical and/or software additions may void the manufacturer's declaration of conformity and may result in the operator bearing full responsibility for the altered device. Such modifications include, among other things, installing additional software of any type, such as antivirus software, or updating or patching components such as the operating system.

2 IT Network Requirements

2.1 Required characteristics and configuration of the hospital IT network

Reference: ISO/IEC 80001 (DIN EN 50173; TIA-568)

The following requirements have to be fulfilled by the customer; otherwise correct function of the AIDA™ isn't guaranteed:

- The availability of a gateway and DNS-Server for the AIDA™ should be ensured
- A minimum bandwidth of 100Mbit/s has to be guaranteed

2.2 Intended information flow between the AIDA™ ME system and the IT hospital network infrastructure

The AIDA™ system supports six types of external servers in the hospital LAN:

2.2.1 Digital Imaging and Communications in Medicine (DICOM)

For further information refer to the AIDA™ "DICOM Conformance Statement"

2.2.2 File Transfer Protocol (FTP)

The AIDA™ system uses passive FTP when exporting data to a FTP server within the IT 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 AIDA™ 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.

2.2.3 Network Share (Server Message Block SMB)

The AIDA™ 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. Therefore 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 AIDA™ 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.

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

2.2.4 HL7 communication (HL7 server / HIS)

The AIDA™ 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.

2.2.5 KARL STORZ OR1™ StreamConnect® 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: White Paper OR1™ STREAMCONNECT® II System

2.2.6 Network Printer

The AIDA™ 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

Note: 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, analyze, and control such risks. This includes any subsequent changes to the network/data coupling introducing new risks and requiring new analysis. Examples of pertinent changes to network/data coupling include:

- Changes in network/data coupling configuration
- Connection of additional items to network/data coupling
- Disconnecting items from network/data coupling
- Update of equipment connected to network/data coupling
- Upgrade of equipment connected to network/data coupling

3 Software Installation

The system is a delivery of a complete system including hardware and software (AIDA™ SW and Windows 7 Embedded).

4 Licensing Model

There is no dedicated licensing model implemented.

5 User Rights

In the AIDA™ ME system, there are three levels of security roles implemented (nurse, hospital it and KST service technician). There is the possibility to set an individual password to the standard AIDA™ user to avoid autologin.

6 Availability

KARL STORZ cannot make any statements regarding the safety and availability of devices that the operator has modified without authorization, for instance, by installing printer drivers, additional software, etc.

7 Availability

KARL STORZ offers remote service for the KARL STORZ devices located in the operating room. Connection between devices in the OR and the Axeda® 3 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 AIDA™ PC only and therefore only the AIDA™ PC 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 AIDA™ PC to allow the network maintenance, monitoring and troubleshooting task via remote service. The access to the system via Axeda® needs the confirmation of the user.

8 Patch Management of the Operating System (OS)

KARL STORZ cannot make any statements regarding the safety and availability of devices that the operator has modified without authorization, for instance, by installing printer drivers, additional software, etc.

9 Malware 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 AIDA™ system is based on Cryptzone 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 Cryptzone 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.

SE46 prevents the exploitation of zero days on OS level and other applications.

Malware protection software may be installed and run under certain conditions. If the operator meets the requirements described below, the appliance's conformity with Medical Device Directive 93/42EEC will remain intact as declared by KARL STORZ.

The operator must configure the software such that it does not limit the operation of the appliance. Please take resource intensive processes, such as video storage during surgery and other real-time applications, into consideration.

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.

10 Data Protection

The AIDA™ system will be used in secured environments like operating rooms or doctors' offices. These are environments with access limited only to selected items.

11 Data Backup and Recovery

This system is not intended to be used as an archive.

The system does not provide a local backup solution. Under normal operating conditions all data will be exported to a defined target after each treatment, which is under customer control as for backups. During a procedure, data is stored locally in a buffer; after the finalization of the treatment an export to predefined targets is initiated. If the export fails, the data export will be resumed after the failure condition has been resolved (e.g. re-establishment of network connectivity etc.)

Data from the current treatment will remain on the local HDD in case of power failure or other adverse events.

12 Network Load

The system can read and write up to 1GBit/sec during storage operations.

13 Network Ports and Protocols

Service	Port
DICOM	Configurable
FTP	20/21
SMB	445
HL7	Configurable
Axeda®	443 and 17002

14 Conformity Assessment

Refer to /REF_002/ for HL7 Interface Description.

15 DICOM Conformance Statement

Refer to /REF_001/ for DICOM Conformance Statement document.

16 Test Protocol

Under certain prescribed circumstances, the Operator may make changes to the KARL STORZ device (e.g. See Section 10, Malware Defense, above). In all circumstances, the Operator is ultimately responsible for risk management in accordance with IEC 80001.

17 System Schematic