ZEISS Remote Service
Security Concept

1. Objective
The objective of this document is to summarize the set of cyber-security controls to ensure medical device cybersecurity for the ZEISS OPMI® PENTERO® 900 and ZEISS OPMI® PENTERO® 800 medical device with an embedded Windows 7 operating system.

2. System overview
The device has the following interfaces which are critical for cybersecurity:

- LAN port for DICOM/PACS interface and ZEISS Remote Service
- USB ports for USB devices
- Touchscreen monitor as graphical user interface (GUI)

3. General principles
Medical device security is a shared responsibility between stakeholders, including health care facilities, patients, providers and manufacturers of medical devices. Failure to maintain cybersecurity can result in compromised device functionality, loss of data (medical or personal) availability or integrity, or expose other connected devices or networks to security threats.

Identification of threats and vulnerabilities

- Malware could re-purpose the system's computing capability if it can access the OS.
- Operators could be tempted to re-purpose the system's computing capability if they can access the OS.
- Malware could expose the device to unauthorized use or alter it.
- Unauthorized access could expose the device to unauthorized use or alter it.

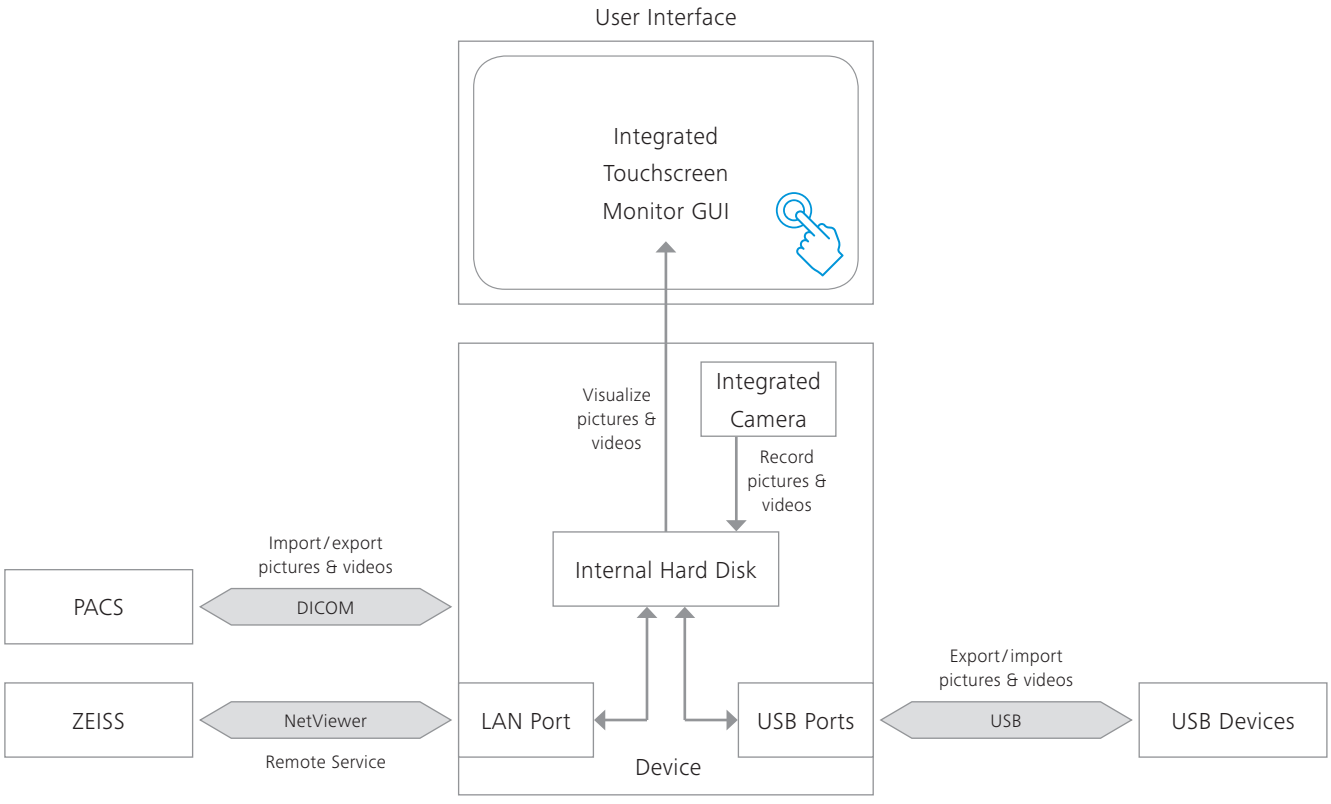

Figure 1: System overview & interfaces

4. Cybersecurity functions

4.1. Limit access to trusted users only

4.1.1. Authentication of users

- For standard users, access to the device is not limited because the device is used only in health care facilities and must be usable in emergency situations (fast access).
- For privileged users, an authentication via password is performed.

4.1.2. Layered authorization model based on the user role

- A layered authorization model with different privileges based on the user role is implemented:
  - Standard users have no access to the configuration of the user rights or to the settings of the IT system.
  - "IT Admin" has additional IT system rights to enable/set passwords for standard users, enable/set up IT connections (DICOM, Remote Service) and set the time and date.
  - "Zeiss Service" user has additional rights to access service dialogs.

4.1.3. Appropriate authentication

- Appropriate authentication is implemented as follows:
  - Standard users do not require any authentication.
  - "IT Admin" requires password authentication.
  - "Zeiss Service" user requires password authentication.

- Password must be entered on a virtual keyboard displayed on the GUI or on an external USB keyboard activated by code. Password authentication via network is not possible.

4.1.4. Strengthen password protection

- "IT Admin" & "Zeiss Service" user authentication passwords are:
  - 17 characters long
  - Device specific

4.1.5. Provide physical locks on devices and communication ports

- Only interfaces which are necessary for the intended use are accessible.
- All other standard PC interfaces are located internally in the device.

4.1.6. User authentication for software or firmware updates

- Software and firmware updates require authentication of the "Zeiss Service" user.
- Hard disk (SSD), where the operating system (OS) and ZEISS application SW is stored, is write-protected. Any unauthorized software can only be installed temporarily and will be deleted after a system reboot.
- BIOS is password protected.

4.2. Ensure trusted content

4.2.1. Restrict software or firmware updates to authenticated code

- Software and firmware updates are only done via ZEISS Field Service Engineers with dedicated configured ZEISS SW update USB sticks.
- All updates require a service password.
- Software checks firmware versions for compatibility.

4.2.2. Use systematic procedures for authorized users to download version-identifiable software and firmware from the manufacturer

- No SW downloads are provided to customers (only to ZEISS Field Service Engineers).

4.2.3. Secure data transfer to and from the device, network integration

- "NetViewer" for remote service with onsite approval. Session initialization can only be started onsite.
- Our surgical microscopes may be integrated within hospital networks for use of the DICOM functionality or remote service access. In this case our system is protected by a firewall with only those ports enabled which are necessary for DICOM communication or remote service access. In addition, remote service access has to be activated explicitly by an IT administrator and is automatically deactivated with the next system shutdown/restart.
- Standardized internationally accepted data transfer protocol: DICOM (not encrypted)

4.3. Detect, respond, recover

4.3.1. Features that allow security compromises to be detected, recognized, logged, timed, and acted upon

- Audit trail, security logs, error logs and user logs are implemented.
- Log files can be exported, encrypted and sent to ZEISS.

4.3.2. Provide information to the end user concerning appropriate actions to take upon detection of a cybersecurity event

- See User Manual page 299 and page 307.

4.3.3. Device features that protect critical functionality, even when the device's cybersecurity has been compromised

- The device magnification and light/illumination features are independent of PC functionality. Both device features can still be used even if the PC is shut down (basic function mode).
- Additionally, a light only mode is implemented to shut down all SW and FW, except the light source, to ensure that the device magnification and light features are available.

4.3.4. Methods for the retention and recovery of device configuration by an authenticated privileged user

- During manufacturing and after each configuration change by a ZEISS Field Service Engineer, a backup is stored.
- ZEISS Field Service Engineers can restore any stored backup.

4.4. Other implemented mechanisms

4.4.1. Protect Windows software system inside medical device

- Customized Windows Embedded Standard 7 (WES7) operating system. Unnecessary components (remote desktop, telnet, etc.) are removed.
- Closed system: our surgical microscopes only grant access to the GUI of the system. There's no possibility of either users or IT administrators gaining access to the Windows operating system. Therefore it is not possible to install additional SW, change or modify existing SW modules which might introduce any viruses or malware to the system or damage it.
- A firewall is installed and activated.
- All unnecessary ports are closed.
- Hard disk (SSD) containing OS and application SW is write protected.
- BIOS is password protected.
- BIOS settings allow only the dedicated internal hard disk (SSD) to be booted. Booting external devices is disabled or requires a BIOS password.
- For all accessible USB ports on our surgical microscopes, the "autorun" functionality is disabled. Therefore a USB device which may be infected by a virus cannot be used to auto execute, activate or upload this virus onto the operating system of the surgical microscope. The system also features a keyboard-lock that prevents unauthorized users (code protected) from starting Windows Explorer from a connected USB keyboard. Furthermore it is not possible to execute any third-party SW application on a connected external USB device which might act as malware, as only FSEs have access to the WES7 operating system and not the user or IT administrator.
- Write protection of the WES7 HDD partition: the WES7 operating system and the ZEISS OPMI PENTERO 900 / ZEISS OPMI PENTERO 800 application software run from a SSD (solid state drive) that has write-protection in place to prevent the installation of unauthorized third-party software applications. Any potential changes by a virus to that partition will be discarded automatically with the next system start. All patient and user data are stored on a second large HDD (1TB) that can easily be replaced in case of hardware malfunction. The OPMI application does not allow other data or executable files to be written to the data partition. Operators can not use the Windows Explorer to create or copy data to that partition.
- It is not possible to execute any third party SW application on a connected external USB device or DVD which might act as malware as the user and IT administrator have no access to the Windows operating system GUI.
- Booting from external device: as the BIOS access for our surgical microscopes is protected by a BIOS password, it is not possible to modify the settings in such a way that the system can be booted from an external USB device or a DVD.

4.4.2. Hide Windows software system inside medical device

- Closed system. It is not visible that Windows software is included in the device. Our surgical microscopes only grant access to the GUI of the application. There is no possibility of either common users or IT administrators gaining access to the WES7 operating system GUI which runs behind the ZEISS OPMI PENTERO 900 / ZEISS OPMI PENTERO 800 application on the GUI. Therefore, it is almost impossible to install and start additional SW, change or modify existing SW modules which might introduce any viruses, malware or harm to the system.
- Startup of BIOS and Windows is hidden by the monitor startup logo.
- No direct access to Windows GUI.
- Application in full screen mode. No Windows desktop.
- Ctrl-Alt-Del does not open Windows Task Manager.
- Windows users “Administrator” and “OPMI user” are password protected and use different passwords.
- “penterouser” is the standard user logged on by the system startup. Log off and switch user functions are disabled.

4.4.3. Protect patient data

- If “Protect patient data” has been activated by the IT administration, standard users can only access patient data after entering their own password. Each standard user must receive their own password.
- Network integration: our surgical microscopes may be integrated within hospital networks for using the DICOM functionality or remote service access. In this case our system is protected by a firewall with only those ports enabled that are necessary for DICOM communication or remote service access. In addition, remote service access has to be activated explicitly by an IT administrator and is automatically deactivated with the next system shutdown/ restart.

5. Summary

The following sections summarize the documentation of the overall design control related to cybersecurity:

A. In risk management, cybersecurity is addressed within the framework of hazard analysis during product development.

B. SW risk mitigation related to cybersecurity

- Remote service only via IT-Admin
- No unnecessary open network ports
- Firewall activated
- No “autorun” for USB and CD/DVD media
- Virus scanner before master image

C. Device instructions for use contain recommendations for cybersecurity control appropriate for the intended use environment (e.g. anti-virus software, use of firewall). See Instruction for Use for the ZEISS OPMI PENTERO 900 / ZEISS OPMI PENTERO 800.

D. For ZEISS OPMI PENTERO 900 / ZEISS OPMI PENTERO 800, no patches will be provided. Necessary SW updates follow the original SW development process. No separate processes for SW update or patches are provided.

E. To ensure that device software maintains its integrity (e.g. remains free of malware), the release candidate software image is checked with an anti-virus program. The software image is stored according to SW Configuration Management. Manufacturing uses an image of SW Configuration Management and checks SW and FW build versions.

A virus scanner can be provided by ZEISS Service upon request.

Carl Zeiss Meditec AG
Goeschwitzer Strasse 51–52
07745 Jena
Germany

EN_37_010_0007II Printed in Germany