CLARUS CYBERSECURITY

Product Security Case Study v1.2

Seeing beyond

1. Introduction

Information Security and Privacy of Medical Devices, also called "Product Security" is an important aspect of their function. It is absolutely necessary to ensure their safe operation, and to ensure:

- Confidentiality of patient data
- Integrity of the Medical Device, essential performance of the device
- Availability of the Medical Device

To ensure Product Security, a Medical Device, has to be designed, implemented and tested properly - but it also needs to be installed, configured, maintained and operated as intended.

If any of these aspects is not observed, the Medical Device's Product Security can be easily compromised, with potential grave consequences for its safety.

The intention of the Product Security Case Study is to ensure that people and institutions responsible for installation, maintenance and operation of Medical Devices have all required information to do their work properly:

- Provide information regarding all relevant Product Security aspects to customer and service personnel.
- Ensure that all data and guidance are available which are required to install, configure, maintain and operate the system securely.

In addition, the Security Case Study is intended to provide all information that may be required during the procurement and selection process for the Medical Device, thus avoiding the need for customer specific questionnaires.

2. Product Security Case Study - Content

The following content should be considered when writing the Security Case Study for any Medical Device, system, software only or other solution. The actual content has to be adapted to the specific nature of the Medical Device in question.

Purpose of this Document

This Product Security Case Study describes the technical aspects of CLARUS that are relevant for Information Security and Privacy and it is mainly intended for the service and customer personnel that are responsible for installation, configuration, maintenance, and operation and for Marketing and Sales to support the procurement process. But it also should be made available to customers on demand for transparency.

This Product Security Case Study contains all required information to:

- Support the procurement and selection process for the product
- Avoid the need for generic security questionnaires
- Securely install, configure, maintain and operate the product

3. System Information

3.1 System Overview

Brief overview of the solution:

3.1.1. Description of Device

CLARUS is an active, programmable electrical medical system which employs Broad Line Fundus Imaging (BLFI) to obtain ultra-widefield high resolution retinal images of the eye human containing structural information and, in the case of the Model 700, vascular flow information. The resulting processed information is used by healthcare providers as an aid in the visualization of ocular structures and an aid in the detection and management of ocular diseases.

3.1.2. Intended Use

The CLARUS 500 and CLARUS 700 ophthalmic cameras are indicated to capture, display, annotate and store images to aid in the diagnosis and monitoring of diseases and disorders occurring in the retina, ocular surface and visible adnexa. It provides true color and autofluorescence imaging modes for stereo, widefield, ultra-widefield, and montage fields of view.

The CLARUS 700 angiography is indicated as an aid in the visualization of vascular structures of the retina and the choroid.

3.2 Hardware Specifications

Operating System	Windows 10 x64 Enterprise 2016 LTSB
Processor	Intel processor with a Passmark benchmark score of at least 5675
Memory	8 GB (CLARUS 500), 16 GB (CLARUS 700)
Internal Storage	900 GB (CLARUS 500), 1800 GB (CLARUS 700)

USB ports	6 ports
Input Devices	KEYBOARD WIRELESS TRACKPAD BACKLIGHT BLKMOUSE WIRELESS LOGITECH MOUSE WIRELESS LOGITECH

3.3 Product Software

3.3.1. Application User Accounts and Management

CLARUS has username and password based authentication for both Windows OS and CLARUS applications.

3.3.1.1. Windows O–S User Accounts and Management

For Windows OS, CLARUS instrument is configured with 3 user accounts:

1. ZEISS - Intended to be used for configuration of OS.
2. ZEISSAdmin - Intended to be used for configuration of OS.
3. Tech Support- Intended to be used by ZEISS Personnel (Tech Support/Field Service).

Standard User accounts can be added and modified by Windows Admin Accounts. It is recommended that Standard User accounts are added and configured for normal user workflows.

All CLARUS application accounts can be run by Windows Administrator or standard user accounts. Standard user accounts have limited privileges using any of the application user accounts (specified in section 3.3.1.2)

3.3.1.2. CLARUS Application User Accounts and Management

For CLARUS application, there are 3 default accounts:

1. Administrator- access to perimeter configuration menus.
2. Service- full access to application software
3. Emergency- access is extremely limited with no ability to view or perform exams on existing patients.

Application Administrator accounts can configure additional application account types- operator and doctor. Multiple accounts with doctor or operator roles can be created. The operator account has access to limited routine operations and doctor account has access to routine operations and the configuration settings.

3.3.2. Audit and Logging

CLARUS Software logs important workflow performed by the user as a part of audit log. It also logs errors and network requests to FORUM and other data sources. Details of these logs are discussed in section 5.5 Event/Audit Logging.

Windows also provides logging for events that are related OS/ Driver/Hardware/Device.

3.3.3. Connectivity

The CLARUS SW supports the following networks and network activities:

- Networking via a local area network or intranet for sharing data between multiple CLARUS instruments and Review Software.
- Archiving to and retrieving from a network file server.
- PACS/EMR connection for storing aquisition data for a secured server.
- USB devices for transferring patient data.
- Printing to networked printer

3.3.4. Software Update and patch

SW can be updated using software upgrade kit by customer or tech support/field service. Only SW provided by ZEISS sources which are signed by ZEISS should be used for install/upgrade.

The software USB includes Windows patches and updates relevant to the current application update only.

NOTE: For access to all approved patches and updates visit the website www.zeiss.com/cybersecurity, or contact customer support.

3.4 Operating System

Configuration of the OS that is shipped with the solution or configuration that the customer is required to provide to run the solution:

3.4.1. OS Version information

- Windows 10 x64 Enterprise 2016 LTSB

3.4.2. Patch level and patch policy

- Automatic Windows updates are disabled. Windows patches and updates are communicated through a monthly newsletter to the SSC after they are tested and approved for use.

3.4.3. Firewall

- The Windows Firewall is enabled by default for all three network profiles (Private, Public, and Domain). Firewall rules have been configured to harden the device. See Enhanced Security settings in IFU.

3.4.4. Network Configuration

CLARUS uses Internet Protocol version 4 (IPv4). CLARUS contains two network controllers. These are named Internal Network (DO NOT CHANGE) and External Network.

Internal Network (DO NOT CHANGE)

Internal network is for instrument use only with the following assignment:

- Static IPv4 address: 192.168.111.3
- Subnet mask: 255.255.255.0

This instrument is not compatible with networks using IPv4 addresses: 192.168.111.2 and 192.168.111.3

3.4.4.1. Required Internal Ports

The network ports listed in this section are required for optimal instrument operation.

Service	TCP	UDP
CLARUS Inter-instrument communication	80	69
CLARUS joystick and focus knob	18081-18082	n/a
CLARUS Iris Cameras	18083	n/a

Table 1: Internal (Computer to micro-controller communication)

Required External Network Ports

Service	TCP	UDP
Database inbound/outbound	80	69
CLARUS Review Software inbound/outbound	3346	n/a
Peer to Peer broadcast inbound/ outbound	n/a	54183
Secure Distributed Data Service inbound/outbound	54188	n/a
Remote file access SMB (Review software in instrument mode and NAS access)	445	n/a
Printer communication outbound	9100	n/a
Remote service HTTP	80	n/a
DHCP	n/a	68
Windows Time Service NTP	n/a	123

Table 2: Required External Network Ports

Required External Network Ports for EMR/FORUM

Service	TCP	UDP
HTTP communication to FORUM outbound	8080	n/a
HTTPS TLS communication to FORUM outbound	8181	n/a
DICOM communication with ZEISS FORUM inbound	11112	n/a
DICOM communication with ZEISS FORUM outbound	11119	n/a
DICOM communication with ZEISS FORUM user configurable outbound	2762	n/a
Forum to device auto-discovery inbound	24500- 24504	n/a
mDNS (Auto-discovery for instruments inbound)		
NOTE: mDNS traffic should not go to the internet from Hospital/ Clinic Firewall	n/a	5353
DCS inbound/outbound	7778	7716-7719, 7700-7703

Table 3: EMR and FORUM

Additional Network Ports

Service	TCP	UDP
Remote service (outbound)	80	n/a

Table 4: Additional Network Ports

Service	TCP	UDP
DHCP	n/a	67 - 68
TCP/IP MS Networking	445	n/a
NTP	n/a	123
NETBIOS Name Service		
(UDP open port visible externally)	137	137
NETBIOS Datagram Service	138	138
NETBIOS Session Service	139	139

Table 4: Additional Network Ports

3.4.5. DHCP requirements

CLARUS utilizes standard windows DHCP functionality. The default DHCP setting is on.

3.4.6. Hardening

- o Enhanced Security: Enhanced Security is a set of hardening controls designed to enhance the security of the instrument by minimizing the exposed attack surface.
  - ■ Devices shipped with CLARUS 1.2 SW have Enhanced Security enabled by default.
  - ■ If there were changes to individual settings or if all enhanced security settings were disabled, the user can re-enable all these settings using the Apply Enhanced Security command in the C:/Drivers Folder, in the Tech Support Windows user account.
  - ■ For devices in the field that are upgraded to CLARUS 1.2 SW, enhanced security is not applied by default. For field upgrades, the customer must run the “Apply Enhanced Security” script. For a listing of all the Enhanced Security controls and instructions on how to enable ES, see IFU.
  - ■ Hardening Script (CLARUS_Hardening.cmd): It is recommended to run the CLARUS Hardening script to apply additional security. The script will enable certain Windows group policies and open/close some network ports. For instructions on how to enable to hardening script, see IFU.
- o Firewall: Windows Firewall is turned on for private and public networks. Many default firewall rules are disabled. See IFU for details on which rules are disabled. Additionally, the Hardening Script will close some network ports.
- o Screen saver/lock screen: The CLARUS is configured to present the Windows lock screen after 15 minutes of inactivity by default. The idle time to lock the screen can be adjusted by the user. A password will be required to log back into the application.
- o Windows Defender: configured and running on the CLARUS. Definition files will be automatically downloaded and installed if the system has internet access.
- o Windows Password rules: The windows password has minimum password length turned on by default. Refer to user documentation for password rules.
- o Tech Support user password: the password for the tech support user is complex and unique for each device, but is static. If desired, the Tech Support user’s password can

be changed, but this may hinder ZEISS support staff from performing service operations.

o Active Directory: CLARUS is compatible with Active Directory integration. This is optional for the user. Refer to IFU to configure CLARUS for active directory.

3.4.7. 3rd Party Software

The following 3rd Party Software are installed on the CLARUS system:

- Printer Drivers
- Acronis True Image

3.5 Connectivity

Description of how the solution connects to its environment and how it interacts with it:

- USB ports: USB ports may be used to connect external storage media for archiving and exporting exam data. Precautions should be taken to prevent the spread of malware when using removable USB storage devices.
- NAS Drives and Shared Folders: NAS drives can be connected and shared folder can be used for data transfer. When using these storage mechanisms, precaution is advised -so that access is not granted to unauthorized users. To enforce encryption between CLARUS and NAS drives, SMB encryption can be enabled. See IFU for further details.
- Bonjour Service: Bonjour is used to auto-connect to FORUM.
- Remote Service Connectivity: ZEISS personnel may use remote service (TeamViewer) to connect to the instrument remotely. See section 5.3 for how remote connectivity is secured.
- TLS is supported for security by DICOM.
- Replication: Replication can be used to synchronize data between CLARUS devices.
- Instrument Mode: Instrument mode can be used to connect a CLARUS device to the CLARUS Review Software.
- Network Printing: CLARUS devices can be configured to securely connect to a printer through a configured network.

3.6 Data Protection

- Database Security: Patient data that resides in a database on the instrument is secured by a secret password. The database itself is not encrypted.
- Image Data Transfer: Image Data Transfers between CLARUS devices or Review Software and Data Archives can be secured through SMB3 encryption.
- Drive Encryption: CLARUS is compatible with BitLocker. BitLocker can be enabled to protect the Operating System and Data partitions.Measures in place to protect sensitive data (e.g. encryption, pseudonymization, anonymization, etc.)
- Exam data access: Access to exam data is restricted to authenticated users.
- Data Export: CLARUS can export data with anonymization of patient identifiers as a DICOM / Image / Movie file.
- DICOM TLS: When enabled, communication between CLARUS and DICOM solution is encrypted so that data is secure. DICOM TLS uses mutual authentication with certificates, both sides must have the certificate (leaf/public key) of the other party in their own trust store.

4. Network Diagram

4.1 Network diagram of the solution

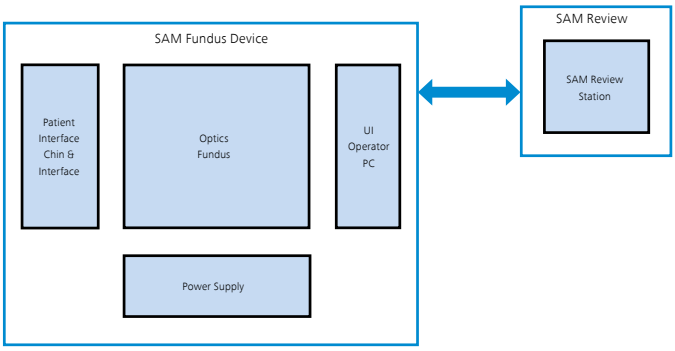
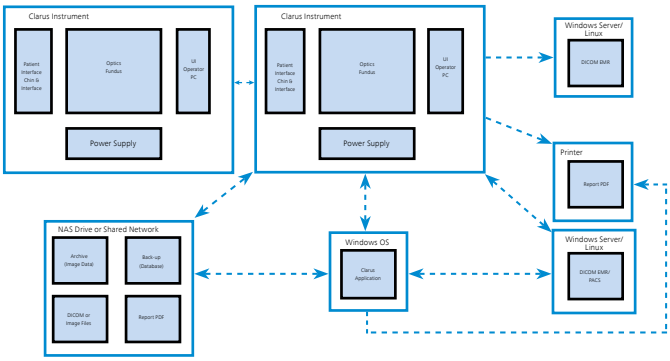


Figure 1: Acquisition Device, Review Station, Archive Systems

4.2 Network diagram of the solution within the customer environment



5. Security Controls

5.1 Security Controls Overview

CLARUS instrument implements authorization and authentication for accounts to secure the device data from misuse. CLARUS instrument also has Windows Defender active. Windows Defender definition files will be automatically downloaded and installed if the system has Internet access. Firewall rules and services are disabled to reduce the attack surface.

5.2 Malware and Vulnerability Protection

- File system protection (e.g. read-only partitions, access rights etc.), firewall and antivirus
- Antivirus: Exception for specific folders defined, to be defined
- Customer supplied antivirus allowed

- Windows defender
- User Account control [enabled optionally]

5.3 Remote Connectivity

N/A

5.4 Authentication and Authorization

Accounts:

Username	Type
ZEISS	Default Windows Account
ZEISS Admin	Default Windows Account
Tech Support	Default Windows Account
Administrator	Default CLARUS Application Account
Service	Default CLARUS Application Account
Emergency	Default CLARUS Application Account
< Operator #1 > …<Operator #2> … <Operator#n>[1]	CLARUS Application Account
<Doctor #1> … <Doctor #2>…<Doctor #n>[1]	CLARUS Application Account

1- The operator and doctor roles are not available by default. An admin application account can create multiple operator and doctor roles as needed by the clinic.

Default accounts Role based access control

Username	Type	Role	Permissions
ZEISS	Default Windows Account	Windows Administrator	Windows Administration
ZEISS Admin	Default Windows Account	Windows Administrator	Windows Administration
Tech Support	Default Windows Account	Windows Administrator	Windows Administration
Administrator	Default CLARUS Application Account	Application's Admin[2]	Change application settings, user management, acquire/analyze data
Service	Default CLARUS Application Account	Application's Admin- used by ZEISS Personnel	ZEISS Technical support
Emergency	Default CLARUS Application Account	Application's operator	Limited operation, unable to view existing patient data
< Operator #1 > …<Operator #2> … <Operator#n>[1]	CLARUS Application Account	Application's operator	Operate device, acquire/analyze data
<Doctor #1> … <Doctor #2>…<Doctor #n>[1]	CLARUS Application Account	Application's doctor	Operate device, acquire/analyze data, change application settings

1- The operator and doctor roles are not available by default. An admin application account can create multiple operator and doctor roles as needed by the clinic.
2- Application Administrator privileges are only available when accessing the CLARUS application from a Windows administrator account.

5.5 Event/Audit Logging

CLARUS creates an audit log entry for the following operations and includes the date/time for each operation:

- Log on/log off
- Create, modify, delete data
- Import/export data from removable media
- Receipt/transmit data from/to the network

Audit logs also record major workflow steps executed by the user throughout their application usage. The audit log also contains the software version and other metadata. A new file is created when the application starts. The events are automatically recorded in (up to) 100 audit files of 10 Mb each. When the maximum limit for files and file size is reached, the device overwrites the existing files. The default folder for the audit log files is D:\Logs. Patient Health Information (PHI) is only available via the audit logs.

Additionally, CLARUS creates an entry in the developer logs for application startup/shutdown, application warnings/errors, and major workflow steps executed by the user. The developer log also contains SW version and other metadata. A new log file is created when the application starts. The events are automatically recorded in (up to) 30 developer log files of 10 Mb each. When the maximum limit for files and file size is reached, the device overwrites the existing files. The default folder for the audit log files is D:\Logs.

Additionally, MySQL audit log logs important information about the device database including logon and transaction information.The default folder for this log is D:/Data/MySQL/Data/CLARUS_mysql.audit.log

The following table provides a summary of the various logs present on the CLARUS system.

File name	Description	Contains Patient Data
Audit.log	Contains operations on patient data.	YES Contains ■ User info ■ All Patient Data
backup-restore.log	Contains all actions of the database backup / restore operations	NO
developer.log	The Developer log contains program specific information e.g. general info method invocations info runtime exceptions and their stack traces.	YES Contains ■ Patient ID
DatabaseAutoRecovery.log	Record the database recovery process	NO
Export.log	Contains information about export status	NO
Import.log	Contains information about import status	NO

File name	Description	Contains Patient Data
nhibernate.log	NHibernate error log. The file size is usually 0 byte.	NO
nim.log	Generated by NIM component. Contains information of DICOM communication with EMR/PACS.	NO Note: May contain patient data if doctor export filepath includes Patient Data
nim-error.log	Generated by NIM component. Contains errors info.	NO
RunAsAdminAudit.log	CLARUS does not use the feature related to this log. The content is empty.	NO
service.log	Contains operations info for FSE trouble shooting.	NO
utility.log	Track when a utility is executed as a separate process. Function name and results are logged	NO

Events like instrument startup, shutdown, security events from Windows Defender, and errors from background applications and database software are also logged in Windows logs. This can be viewed in Event Viewer on Windows 10. The logs are retained and can be removed by admin user.

5.6 Disaster Prevention and Recovery

Description of all disaster prevention and recovery features and measures, including:

- Backup and restore mechanism: Customer can make a backup of database or manually export data to a NAS drive or external media (e.g. Network Shared folder).
- Acronis Backup: An operating system image can be applied to reset a device to factory settings.
- PACS Archive System: User can archive all data to a PACS system. Data on the device will be purged after 14 days of inactivity.
- Native Archive System: Image data can be stored in a NAS drive. Data on the device will be purged after 14 days of inactivity. The device can be configured with multiple archives.

5.7 Security / Privacy Design Approach

At ZEISS, the security and privacy of our product are at the core of development process. All products are developed in accordance to our secure software development lifecycle processes. Following such practices help us reduce the number of vulnerabilities in released software, reduce the potential impact of the exploitation of undetected or unaddressed vulnerabilities, and address the root causes of vulnerabilities to prevent future recurrences.

ZEISS's Secure SDLC (Software Development Life Cycle)consists of the following processes:

- Threat Modeling
- Static Application Security Testing (SAST):
  - We conduct routine security code scans to analyze product source code and application behavior to detect error-prone practices. These tools cover issues ranging from improper management of memory to error prone database query construction (e.g., unescaped user input leading to SQL injection). When issues are identified, we perform root-cause analysis to systemically address vulnerabilities.
- Software Composition Analysis is executed for the product.
- Penetration Testing: Penetration testing is conducted to help ensure CLARUS devices are secure according to industry best practices.
- Information Security Risk Assessment for Products
- Cybersecurity assessment: Cybersecurity Assessment for CLARUS has been performed. Assets, impairments, and vulnerabilities have been identified. Risk is evaluated for those threats and mitigation measure(s) are identified. These measures are logged as system/software requirements.