ELEKTA

Product Security Statement for Leksell Gamma Knife® Perfexion™ version 10.2

1   Summary

Leksell Gamma Knife Perfexion is designed for safety with high levels of redundancy on both hardware and software. Checksums are used on both configuration and patient data to assure data integrity. A special software solution, the Computer Integrity System (CIS) is used to assure that only certified code is allowed to execute on the MCU computer, making mistreatment due to a virus attack virtually inconceivable.
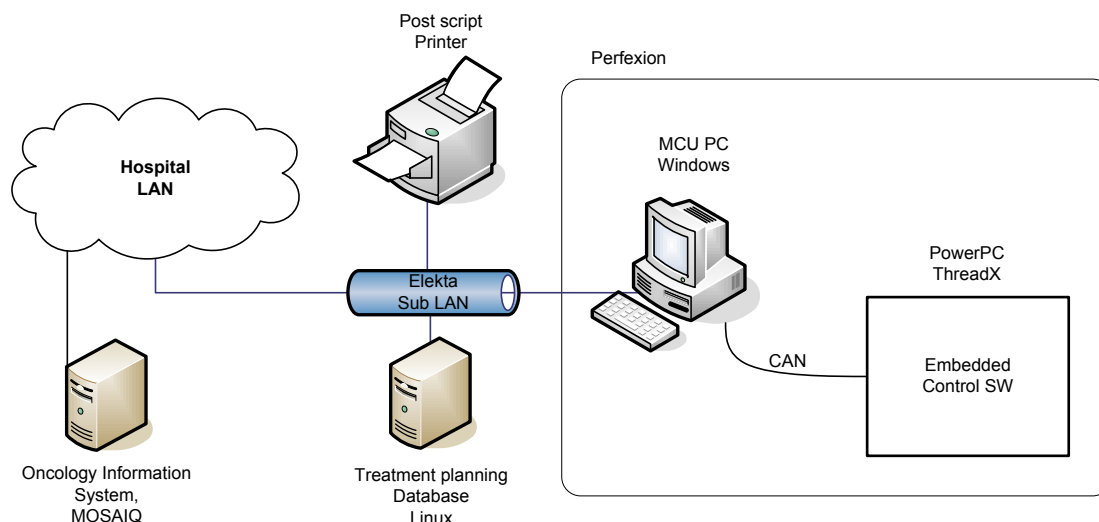
The computer integrity function also prohibits malicious software from spreading between the Elekta system and the hospital network.

All application users are identified and activities are logged.

2   Product Description

Leksell Gamma Knife Perfexion and the Leksell GammaPlan© treatment planning database form a sub network that can be connected to the hospital network. The Leksell Gamma Knife Perfexion workflow can optionally be integrated to the oncology information system, MOSAIQ.

The product's software consists of two parts communicating over CAN using a proprietary application protocol.

2.1   MCU Software

- The MCU software implements the user interface for Leksell Gamma Knife® Perfexion.
- The application software is running on Windows XP on a rack mounted industrial PC.
- The MCU connects to the treatment planning database via the Dataflow Manager (DFM). The DFM is running on the same workstation as the database. The database node is also used for time synchronization via NTP.
- The MCU uses a network postscript printer to print reports.
- The MCU PC has support for connecting a USB memory stick that is used to export reports and log files.

2.2   Embedded Control Software

- The embedded software controls and supervises all system activities during the actual treatment process.
- The embedded software is installed on the ThreadX operating system on two separate Power PCs situated in the Perfexion control system cabinet. One Power PC controls all motions using servos and actuators, the other supervises that all motions are carried out according to the treatment plan.
- The embedded SW is stored on persistent memory in the embedded part of the system and loaded upon power up and is automatically reloaded after an error.

3   Software Security Features

3.1   Computer integrity

The installed Computer Integrity System (CIS) addresses the virus issue by verifying every single file before it is allowed to execute on the system. The system is built on the concept of Application Certificates. These are used to create system specific policy certificates that states exactly which programs are permitted to run. This will effectively hinder all unwanted activities on the protected Leksell Gamma Knife Perfexion MCU computer including;

- ShellScripts (.bat, .cmd etc)
- DOS binaries
- Windows binaries
- Visual Basic for Applications
- Visual Basic scripting

- Javascripts
- Java class file

The Leksell Gamma Knife Perfexion application starts automatically upon powerup and settings are adopted in order to block user access to the Windows OS.

The Windows firewall is active on the MCU, enabling one port for Elekta Service local access.

3.2   Application data integrity

All application configuration and calibration data is stored in the MCU. These files are protected by a checksum. The data is transferred to the embedded control software upon startup.

The treatment data is read from a specific read only part of the Linux based treatment planning database (Leksell GammaPlan).

There is no encryption of the data in the database, however the treatment data imported to Perfexion is protected by a checksum. After a treatment plan has been loaded from the treatment planning database it is sent to the embedded control software.
The MCU application redundantly supervises that the treatment plan in the database is equal to the treatment plan loaded in the embedded part of the system.

All messages on the interface between the MCU and the embedded part contain checksums to ensure error free reception.

No parts of the MCU file system is shared on the network.

3.3   User identification

Logon to Windows on the MCU PC is automatic using the only available account.

Logon to the MCU application requires user name and password.
There are three types of users:
- Certified users: User account with full access to all functionality in the clinical mode, including starting a treatment. User administration rights of Certified and non-certified users.
- Non-certified users: Other medical personnel with limited access to the functionality in the clinical mode. Among other things, they are not allowed to start a treatment. These users have NO user administration rights.

- Service users: Elekta service personnel with full access to all functionality in the service mode. Service Users are not allowed to start a treatment. User administration rights of all types of users.

4 Your responsibilities for Security

4.1 User administration

You are expected to administer both Certified and Non Certified user accounts.
To increase the security of your product it is recommended that you introduce a local procedure for password policies.

4.2 Network

For best performance and reliability it is recommended that the Primary Leksell GammaPlan workstation, the MCU and printer are connected direct to the supplied switch forming the Elekta sub network.