Patient QA with myQA SRS Detector CyberSecurity Leaflet

The purpose of this leaflet is to provide CyberSecurity information on the myQA SRS Detector and myQA Patients software for IT personnel.
This information will help ensure the secure and safe use of the system in clinical practice.

What is the system used for?

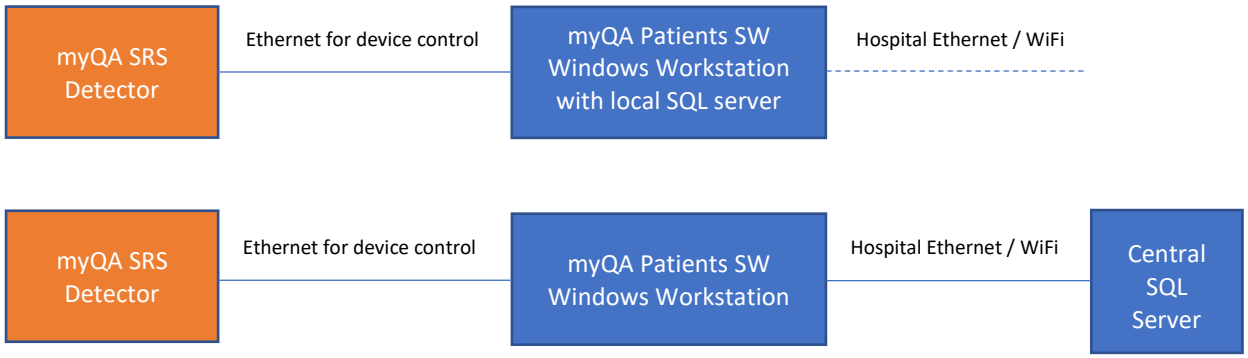
For cancer treatment, Linear accelerators apply treatment plans to a patient, by delivering a Dose with different energies, patterns and from different angles.

- The purpose of the system is to record a simulated treatment and to compare it versus a treatment plan.
- The myQA SRS Detector is placed on the couch instead of a patient, and the treatment plan is applied. The device records the treatment dose distribution and corresponding angles. The result is compared to the plan in the myQA Patients software. If there are significant deviations, it can be assumed, that the plan cannot be delivered to a patient as expected. The plan will be recomputed, or the Linear accelerator will be checked for errors.

What if the measurement device fails or measured data is corrupted?

In this case, the comparison of recorded treatment vs. plan will fail, the patient will not be treated, and the medical physicists will start a root cause investigation.

How does the system architecture look like?



Are there any operating systems or application software supplied?

The myQA SRS Detector is used with the myQA Patients Software package which is delivered together with the detector. The myQA Patients Software also contains the IBA software interface to the myQA SRS Detector.

There are no operating systems delivered in the standard package.

- The myQA Patients Software package runs on Hardware / OS provided by the hospital IT.
- The myQA SRS Detector contains a FPGA and a frame grabber to control and read the measurements.

In some situations, the connection of an “interface module” between the workstation and the SRS Detector becomes necessary, improving the network traffic to avoid lost frames. This interface module:

- is a commercially available industrial computer, such as e.g. Lenovo ThinkEdge SE30, equipped with a Windows IoT operating system,
- is installed between customer’s PC and the SRS Detector,
- contains the myQA SRS Adapter software and the uniformity correction file(s) belonging to the individual SRS Detector connected.
- The procedure of how to enable Remote Desktop in order to install (security) updates of the Windows IoT operating system and of the myQA SRS adapter software is described in a technical note accompanying the interface module.
- This interface module is supposed to be operated under the custody of the hospital IT and all precautions must be applied as required by local cybersecurity policy.

What kind of data is stored and handled?

- The myQA Patients Software package handles patient related data, including data which is used to identify the patient (such as name, date of birth). This data is saved in the SQL database.
- The myQA SRS Detector stores the following data:
  - Configuration data.
- The myQA Workstation stores the following data:
  - Calibration and Uniformity Correction files.
  - Software error logs.

- The Central SQL Server stores the following data:
  - Measurements acquired with the myQA SRS Detector.
  - Treatment Plans imported from the Planning System.
  - Comparison / plan verification results.
  - Pass / Fail decisions.
  - Patient related data (as mentioned above).
  - Event logfile (audit log).
- The following data are transmitted between workstation and myQA SRS Detector:
  - Measurements acquired with the myQA SRS Detector.
- The following data are transmitted between workstation and SQL data base:
  - Measurements acquired with the myQA SRS Detector.
  - Treatment Plans imported from the Planning System.
  - Comparison / plan verification results.
  - Pass / Fail decisions.
  - Patient related data (as mentioned above).
  - Event information (stored in the audit log).
- Ports:
  - myQA Patients: the port for the DICOM listener is 998, and configurable by the user.
  - myQA Cockpit: this viewer application uses port 52803 which is configurable by the user.
  - myQA SRS Adapter: the default port is 53535, and configurable by the user.
- Encryption
  - All data which is used to identify the patient (such as name, date of birth) is encrypted in the SQL database. This also applies to the event logfile.

Interfaces

- DICOM interface, used for the import of patient treatment plans.
- Import of “path.xml” files in case a Cyberknife system is used.
- If the optional viewer application myQA Cockpit is used, particularly when used from outside the clinical premises, it is strongly recommended to secure the connection between myQA Cockpit and the SQL server either by a VPN or by TLS 1.2 / 1.3.

Which measures are implemented by IBA Dosimetry to support safe and secure operation?

- All patient personal related data are encrypted.
- Access to SQL server requires authentication.
- User authentication for the myQA Patients Software package, requiring the use of strong passwords.
- Use of TCP/IP as transport protocol.
- Communication between workstation and myQA SRS Detector uses our proprietary Hermes protocol and is secured with TLS.
- Both factory calibration and user uniformity correction files are secured with a hash value.
- Event logging (audit log) for patient related operations (Read, Write, Update, View, Backup / Restore).
- The connection to the optional viewer application myQA Cockpit can be secured with TLS 1.2 or 1.3.
- MDS-2 forms are published for both the myQA SRS Detector and the myQA Software package, and are available from our customer support team.
- Updates to the myQA Patients Software package are protected with a hash value (SHA-256). This hash value can be used to verify the authenticity of the update file received.
- Our source code is continuously scanned for vulnerabilities using SonarQube.
- The installers have a digital signature.

Which CyberSecurity measures are expected to be implemented by the operator (health care provider)?

- General requirements expected:
  - State of the art virus scanners and firewalls for the tablet and PC are used.
  - Prescribed maintenance is done as required, including installation of security patches.
  - Windows session timeout for web application session is configured according to local policy.
  - Access control to the medical devices and network access points is established (physically and electronically). Internet access is appropriately protected.
  - An Adequate password policy is implemented.
- Device specific:
  - Setting up an isolated network between workstation and myQA SRS Detector is required to avoid cybersecurity risks and performance issues.
- While no CyberSecurity issues are known at the time of release of the Dose-X we cannot completely rule out that in the future previously unidentified vulnerabilities or security issues might arise. It is therefore recommended that the customer's risk management team performs a risk assessment related to the use of the device and the myQA Software in the IT network.

We care: what happens in the case of a CyberSecurity incident?

- IBA Dosimetry is available for you 24/7. We welcome any notification about any CyberSecurity event or suspected vulnerability involving IBA hard- or software products.
- Please feel free to call our customer support team or file a request in our helpcenter (see contact information and link below).
- We will handle such reports with high priority, and you will be continuously informed about the progress. If necessary, we will publish a security patch.