iqmessenger

# Maximum availability with end-to-end supervision

March 2020

# Redundancy and end-to-end supervision IQ Messenger

The IQ Messenger software platform for critical messaging and communications provides various measures to provide maximum availability and reliability. Permanent end-to-end supervision with connected (medical) devices and systems is hereby realized. Unparalleled performance and system availability are expressed in an 99,99% uptime using the IQ Messenger platform in a redundant mode. This evidence based uptime is part of our ISO13485 certification and annual notified body audit.

The following mechanisms and functionalities are incorporated in the IQ Messenger platform to ensure a maximum uptime and availability:

1 *Redundancy with automatic server failover of the IQ Messenger platform*
2 *End-to-end supervision of all connected medical and non medical devices*
*Supervising the (medical) devices providing alarms, all the way to our SmartApp running on the smart devices used by the healthcare professional*
3 *Monitoring of the IT network by IQ Messenger (two-way monitoring)*
4 *External autonomous watchdog monitoring, part of the NEN2575 standard for fire alarm*
5 *Queue mechanism of the nurse call system and medical systems in case of network failure*

## IQ Messenger cluster (also known as high availability or redundancy)

The IQ Messenger software runs within an High-Availability (HA) cluster environment on two different (virtual) servers. If there is a disruption of the server or one of the critical applications of the IQ Messenger software, the second server will take over the operation automatically.

## Failover

When one or more of the critical services are failing on the first server, this server will attempt to autonomously restore the relevant processes. If this does not happen within a variable time, the second server will take over the sessions and act as the primary server. An alarm message is also send to a device or system of choice for notification.

A failover of the redundant server takes about 10 seconds. When medical devices have an alarm during the failover time, they are automatically placed in the alarm queue of the medical device itself or the current status of the medical device is updated. This logic therefore differs per medical device and no messages are lost as they will be resend by the medical device or retrieved by the IQ Messenger platform.

### Example with a BBraun infusion pump:

BBraun does not send alarm messages to IQ Messenger, Instead, IQ Messenger must request the current status / alarms of the device every 5 seconds using the specific BBraun BCC protocol. If IQ has a failover, the connection to the medical device is immediately restored by the other server and the current status is requested again. If an alarm has occurred in the meantime, the status of the pump has changed and is read out by the IQ Messenger platform. The event / alarm retrieved from the BBraun device will inmediately trigger an eventflow in the IQ Messenger platform notifying (healthcare) professionals and or activating other third party systems.

### Example with a Philips patient monitor:

The Philips Emergin gateway / server receives the alarm messages from the Philips monitors and sends them to IQ Messenger using the supervised OAP protocol. In this case IQ Messenger does not request the alarm messages but receives them from the Emergin gateway. In the event of a failover of the IQ Messenger server, the message is stored in the queue of Philips Emergin, since Emergin does not receive an acknowledge from IQ Messenger on its send alarm message. When the connection between IQ Messenger and Emergin is restored, Emergin sends its messages from it's queue directly to IQ Messenger, triggering an eventflow.

### Medical devices:

Apart from retrieving or receiving alarm messages, there is a second communication way with the medical device, the heartbeat. In case of BBraun we request a heartbeat every 5 seconds and with Emergin we receive an OAP heartbeat message every 15 seconds. It is possible that the network in the hospital or the medical device has a short disruption resulting in a heartbeat message being missed by the IQ Messenger platform.
To prevent unnecessary alarm fatigue and irritation upon employees, IQ Messenger has developed a suitable mechanism in consultation with hospitals. A heartbeat loss is only considered in case of three consecutive missed heartbeats. In that case an alarm / eventflow is triggered by the IQ Messenger platform informing professionals and or activating third-party systems.


## SmartApp:

The SmartApp application running on Android smart devices is also equipped with supervision. That means that the device / SmartApp itself detects when the heartbeat to the IQ server has been disconnected.

The healthcare professional is informed (acoustically and visually) about the connectivity status of her device.

The IQ Messenger server itself also monitors the heartbeat with the devices / SmartApps and can also send alarms / events when a smart device has been disconnected. Consider informing a central operator, a manager or in case of compliance with the NEN2575 fire safety legislation.
A two-way supervision between the IQ Messenger platform and the smart devices is achieved.

## Network:

We can now conclude that there is complete end-to-end supervision from the source of the alarm (medical device, nurse call system, personal alarms, etc.) all the way to the smart device / SmartApp used by the professional. The IT network of the hospital acts as a "transport layer" enabling IQ Messenger to receive and send alarms from and to third-party systems. The IQ Messenger platform is therefore capable of monitoring the intermediate IT network and all its servers, routers, switches, etc.

Based on our own experience as well as indicated in our presentation of the 'Koepelorganisatie MIT' at the 'Zorg & ICT' trade-fair, the vast majority of disruptions within an (medical) alarm environment can be traced back to the performance and human errors related to the IT network. In most cases IT network issues can be avoided. The hospital must provide a performing and reliable IT network (state-of-the-art) in which only qualified professionals are allowed to execute maintenance using clear and safe procedures and control measures.

### Two-way monitoring:

Unlike traditional nurse call systems or alarm servers, the important services / components that "run" within the IQ Messenger platform can also be monitored by the hospital itself using a standard SNMP application.
Now the performance of IQ Messenger is not hidden in a "black box" or in a sales and marketing expression, but transparent and measurable using standard tools by the hospital itself. The end-to-end supervision is also being expanded with our two-way monitoring of the hospital IT network.

### Watchdog:

Apart from the functionality above, a watchdog feature can also be implemented. By using an autonomous Wago dry contact input/output module, a lamp, flash, horn, etc. can be activated in case of an important network or third-paty system failure. The watchdog functionality is always used in a certified NEN2575 fire alarm environment.

IQ Messenger B.V.
Pieter Zeemanweg 57
3316 GZ Dordrecht
www.iqmessenger.com