Redundantie en ketenbewaking IQ Messenger

Januari 2020

Redundantie en ketenbewaking IQ Messenger

Het IQ Messenger platform voorziet in diverse veiligheidsmaatregelen om te voorzien in een maximale beschikbaarheid en betrouwbaarheid waarbij de connectie met aangesloten apparaten en systemen permanent wordt bewaakt. De betrouwbaarheid van het IQ Messenger platform wordt in redundante versie (zie onderstaande tekening) uitgedrukt in een uptime van 99,99% en is als zodanig ook opgenomen in onze ISO13485 certificering.

De onderstaande mechanismen en functionaliteiten kunnen als volgt worden samengevat:

1 *Redundantie met automatische fail-over van het IQ Messenger platform*
2 *Ketenbewaking van de op IQ Messenger aangesloten (medische) apparaten. Bewaking van alarm bronapparaat tot en met het device waarop het alarmbericht wordt afgeleverd*
3 *Bewaking van het IT netwerk door IQ Messenger (kruislinkse bewaking)*
4 *Bewaking van IQ Messenger door het IT netwerk (kruislinkse bewaking)*
5 *Externe autonome watchdog bewaking, onderdeel van de NEN2575 norm*
6 *Queue mechanisme VOS en medische systemen bij netwerk uitval*

IQ Messenger cluster (ook wel high availability of redundantie genoemd)

De software draait binnen een HA cluster omgeving op twee verschillende (virtuele) servers. Indien er een verstoring is aan de server of een van de kritische applicaties van de IQ Messenger software zal de andere (slave) server de werking automatisch overnemen.

Fail over

Wanneer een of meerdere van de boven genoemde services op de master server zijn verstoord wordt probeert de master server eerst het betreffende proces autonoom te herstellen. Wanneer dit niet binnen een variabele tijd gebeurt zal de slave server de sessies overnemen en fungeren als master. Tevens wordt een alarmbericht naar een device of systeem van keuze uitgestuurd ter kennisgeving.

Een fail over van de redundante server duurt ca 10 seconden. Wanneer medische apparaten in die fail-over tijd een alarm hebben worden deze automatisch in de alarm queue van het medisch apparaat zelf gezet of de actuele status van het medisch apparaat wordt vernieuwd. Deze logica verschilt dus per medical device en er gaan geen berichten verloren.

Voorbeeld met een BBraun infuus pomp. BBraun stuurt ons geen alarmberichten middels haar BCC protocol maar IQ moet om de 5 seconden de actuele status/alarmen van het apparaat opvragen middels dit BCC protocol. Indien IQ een fail-over heeft wordt de connectie met het medical device door de andere server direct hersteld en de actuele status opnieuw opgevraagd. Heeft er in de tussentijd een alarm plaatsgevonden is de status van de pomp gewijzigd en wordt deze door IQ uitgelezen en vervolgens een event/alarm flow in werking gesteld.

Voorbeeld met een Philips patiëntmonitor. De Emergin server ontvangt de alarmberichten van de Philips monitoren en stuurt deze middels het bewaakte OAP protocol aan IQ Messenger. De alarmberichten vragen we dus niet op maar krijgen we toegestuurd. In geval van een fail-over van de IQ Messenger server wordt het bericht in de queue van Philips Emergin bewaard, Emergin krijgt immers geen acknowledge op haar verzonden alarmbericht. Wanneer de connectie tussen de IQ Messenger en Emergin is hersteld na de fail-over stuurt Emergin alsnog haar berichten uit de queue direct aan IQ Messenger.

Medical devices/medische apparatuur:

Los van het ophalen of ontvangen van alarmberichten is er nog een tweede communicatie met het medical device, de heartbeat. In geval van BBraun vragen wij om de 5 seconden een heartbeat op en bij Emergin ontvangen wij per 15 seconden een OAP heatbeat bericht. Nu kan het zijn dat het netwerk in het ziekenhuis of het medical device een korte verstoring heeft waardoor er een heartbeat wordt gemist. Om irritatie en onnodige belasting van de medewerkers te voorkomen heeft IQ hier een passend mechanisme in samenspraak met ziekenhuizen voor ontwikkeld. Pas wanneer IQ drie heartbeats achter elkaar mist wordt een alarm/event getriggerd.

SmartApp:

Ook de SmartApp Android kent een volledige bewaking. Dat wil zeggen dat het toestel/SmartApp zelf detecteert wanneer de heartbeat naar de IQ server voor welke reden dan ook is verbroken. Dit wordt zowel akoestisch en optisch op het toestel weergegeven. Zo weet (hoort en ziet) de verpleegkundige altijd wanneer ze op het toestel kan vertrouwen en wanneer niet.

Tevens bewaakt de IQ server zelf ook de heartbeat met de toestellen/SmartApps en kan vervolgens ook alarmen/events versturen wanneer er een toestel geen connectie meer heeft. Denk aan het informeren van een centralist, een leidinggevende of in geval van compliance aan de NEN2575 brandmeld wetgeving.

Netwerk:

Uit het bovenstaande kan je dus opmaken dat er sprake is van een volledige ketenbewaking vanaf de bron van het alarm (medical device, VOS, persoonlijke alarmering etc) naar het toestel/SmartApp. Het IT netwerk van het ziekenhuis ligt hier als "transportlaag" tussen. IQ gaat hier nog een belangrijk stuk verder. Zo kunnen wij ook het tussenliggende netwerk en al haar servers, routers, switches, etc bewaken.

Zoals ook in onze presentatie van de Koepelorganisatie MIT op de Zorg en ICT beurs aangegeven is het overgrote deel van verstoringen te herleiden naar de performance en menselijke fouten binnen het IT netwerk. Te kritische alarmtimers zijn dan ook vaak "niet werkbaar" binnen ziekenhuizen. Het ziekenhuis dient op haar beurt een geschikt en betrouwbaar IT netwerk ter beschikking te stellen waarbij uitsluitend gekwalificeerde professionals middels duidelijke en veilige procedures onderhoud mogen uitvoeren.

Kruislinkse bewaking:

In tegenstelling tot traditionele VOS systemen of alarmservers kunnen de belangrijke services/componenten welke "draaien" binnen IQ ook door een standaard SNMP applicatie van het ziekenhuis zelf worden bewaakt.

Zo is de performance van IQ niet verborgen in een "black box" of in een marketinguiting maar transparant inzichtelijk en meetbaar door het ziekenhuis zelf. Tevens wordt de ketenbewaking verder uitgebreid met een kruislinkse bewaking van IQ en het netwerk.

Watchdog:

Los van het bovenstaande kan ook nog een watchdog functionaliteit worden ingezet. Middels de inzet van een autonome Wago contactmodule kan er bijvoorbeeld een lamp, flitser, hoorn etc worden ingeschakeld wanneer het gehele systeem incl. netwerk uitvalt. De watchdog wordt altijd ingezet in een NEN2575 brandmeld keten.

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