Um die Erstfehlersicherheit zu erreichen, werden medizinische elektrische Geräte häufig mit zweikanaligen Architekturen ausgestattet. Doch es gibt alternative risikomindernde Maßnahmen.

Alternativen für zweikanalige Sicherheitsarchitekturen

Mit der Sicherheit von Medizinprodukten ist es so eine Sache. Einerseits muss ein höchstes Maß an Sicherheit integriert werden, um die geforderte Erstfehlersicherheit von Medizinprodukten gemäß EN 60601-1 zu erreichen. Andererseits spielen auch wirtschaftliche Aspekte eine Rolle, die die Auswahl und den Einsatz von risikomindernden Maßnahmen beeinflusst.

Medizinprodukte mit zweikanaligen Architekturen auszustatten, stellt eine weit verbreitete Methode dar und ist zunächst einmal keine schlechte Idee, erhöht jedoch unter Umständen die Komplexität eines Systems. Darüber hinaus fallen in der Regel auch die Material- und Herstellkosten bei zweikanaligen Systemen oder Subsystemen höher aus. Es stellt sich daher die Frage, ob eine vergleichbare Sicherheitsintegrität auch mit weniger Aufwand zu erlangen ist, oder, um der Sache noch mehr auf den Grund zu gehen, ob eine Zweikanaligkeit für das zu entwickelnde Medizinprodukt überhaupt erforderlich ist. Allgemeingültige Antworten gibt es leider nicht. Mit etwas Entwicklungserfahrung und einer systematischen Vorgehensweise, die auf einem Risikomanagement-Prozesses gemäß EN ISO 14971 beruht, lassen sich allerdings individuelle Lösungsansätze erarbeiten. Der Startpunkt bildet dabei die Risikoanalyse, die unter anderem die Betrachtung möglicher Fehler in den verschiedenen Funktionsblöcken eines Medizinproduktes sowie die Analyse der daraus resultierenden Gefährdungen beinhaltet. Mit der Bestimmung der Schweregrade und der Auftretenswahrscheinlichkeiten der Schäden, können daraufhin die Risiken der jeweiligen Gefährdungen bzw. der Gefährdungssituationen beurteilt werden. In einem nächsten Schritt folgt dann die Auswahl der risikomindernden Maßnahmen.

Bei diesen aufgeführten initialen Analysetätigkeiten entstehen unter anderem zwei essentielle Fragestellungen: (1) Welche möglichen Fehlerursachen müssen bei der Betrachtung von Gefährdungen überhaupt angenommen werden und (2) welche risikomindernden Maßnahmen sind ausreichend, um die Erstfehlersicherheit zu gewährleisten? Antworten findet man auf beide Fragen in der EN 61508-2, die als Sicherheitsgrundnorm zwar einen Stand der Technik darstellt, auf Medizinprodukte streng genommen jedoch nicht anwendbar ist. Es gibt allerdings kaum eine vergleichbare Quelle, die in einer ähnlichen Form funktionsbezogene Ausfallarten sowie zugehörige risikomindernde Maßnahmen in einer recht übersichtlichen Darstellung bietet inklusive einer Aussage über deren Wirksamkeiten.

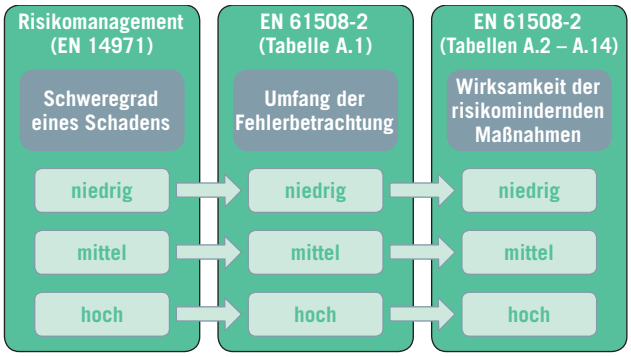
In Tabelle A.1 der EN 61508-2 sind verschiedene elektronische Komponenten mit möglichen Fehlerursachen aufgeführt, die bei einer Fehlerbetrachtung herangezogen werden müssen [Tab. 1]. An diskreten Bauteilen und Sensorik-Baugruppen sind beispielsweise Stuck-at-Fehler, offene Ausgänge und Ausgänge mit hoher Impedanz, Kurzschlüsse zwischen Signalleitungen sowie Drift und Oszillation zu betrachten. Allein schon aus der Vielzahl der möglichen Fehler lässt sich erahnen, dass ohne zu-

Bauteil / Komponente	Tabelle	Schweregrad eines Schadens		
		niedrig	mittel	hoch
Diskrete Hardware	A.3 A.7, A.9	stuck-at	stuck-at; Kurzschluss;Unterbrechung, Drift; Oszillation	
Sensoren	A.13	stuck-at	stuck-at; Kurzschluss;Unterbrechung, Drift; Oszillation	
Veränderlicher Speicher	A.6	stuck-at bei Daten/Adressen	stuck-at; Soft-Errors; ...	stuck-at; Soft-Errors; dyn. Kopplung; ...
Taktquellen	A.11	Sub-/Super- harmonische; Jitter	Falsche Frequenz; Jitter	
Kommunikation	A.12	falsche Daten / Adressen; keine Übertragung	alle Fehler, die Daten beeinflussen; falsche Daten / Adressen; falsche Übertragungszeit / -reihenfolge	

Tab. 1: Fehlerannahmen für zufällige Hardware-Ausfälle (in Anlehnung an EN 61508-2; Tabelle A.1)

risikomindernde Maßnahmen	Verweis EN 61508-7	Schweregrad eines Schadens / Wirksamkeit
Überwachung während des Betriebs	A.1.1	niedrig/mittel
Analogsignal-Überwachung	A.2.7	niedrig
Dynamische Prinzipien	A.2.2	mittel
Hardware mit automatischen Tests	A.2.6	hoch
Überwachte Redundanz	A.2.5	hoch
Testmuster	A.6.1	hoch
Referenzsensor	A.12.1	hoch

Tab. 2: Struktur der Tabellen A.2 – A.14 für risikomindernde Maßnahmen (in Anlehnung an EN 61508-2; Tabellen: A.3 für elektronische Bauteile und A.13 für Sensoren)



Tab. 3: Zusammenhang zwischen Schweregrad eines Schadens, Umfang der Fehlerbetrachtung und Wirksamkeit von risikomindernden Maßnahmen

sätzliche risikomindernde Maßnahmen mit einer einkanaligen Architektur eine Erstfehlersicherheit nicht erreicht werden kann. Allerdings muss nicht jeder Fehler zu einem Schaden führen und das Schadensausmaß kann auch von Fehler zu Fehler unterschiedlich sein. Folglich kann der Schweregrad eines Schadens als grundlegende Größe für die Fehlerbetrachtung sowie die Auswahl von risikomindernden Maßnahmen herangezogen werden.

Mit dieser Sichtweise kann man nun wieder auf die Tab.1 in Bild 1 zurückgreifen. Die zu betrachtenden Fehlerarten sind in die Stufen „niedrig“, „mittel“ und „hoch“ aufgeteilt, die sich auf die Anforderungen des beanspruchten Diagnosedeckungsgrades beziehen. Der Diagnosedeckungsgrad soll an dieser Stelle nicht näher erläutert werden und wird stattdessen mit dem Begriff „Schweregrad eines Schadens“ als Maß der möglichen Auswirkung einer Gefährdung in Bezug auf das Risikomanagement bei Medizinprodukten ersetzt. Je höher also der Schweregrad eines Schadens ist, desto umfangreicher sollten Fehler, beispielsweise in einer FMEA, betrachtet werden. In Risikoanalysen werden meist mehr als drei Stufen für die Schweregrade von Schäden verwendet, für die im nächsten Schritt folgende Auswahl von risikomindernden Maßnahmen reichen aber die drei Stufen in der Tabelle A.1 als Anhaltspunkt vollkommen aus.

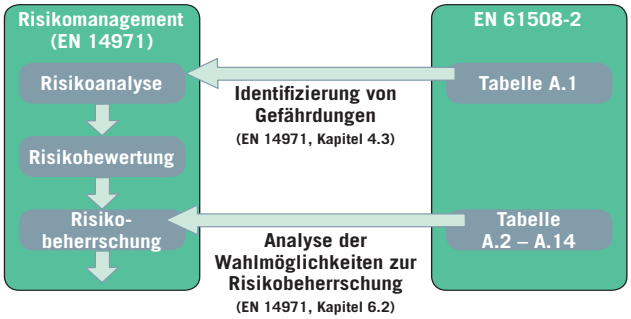
Aus der Tab.1 erhält man nicht nur einen Hinweis auf die in einer Risikobetrachtung anzunehmenden Fehler, sondern in der zweiten Spalte auch einen Verweis auf weitere insgesamt dreizehn Tabellen, in denen passend zu den verschiedenen Komponenten, diverse Möglichkeiten für die Risikominderung aufgezeigt werden [Tab. 2]. Auch in diesen Tabellen kann die Begrifflichkeit des „Diagnosedeckungsgrades (DC)“ mit dem „Schweregrad eines Schadens“ ersetzt werden, wobei die drei Stufen „niedrig“, „mittel“ und „hoch“ vor allem als Maß für die Wirksamkeit der jeweiligen Maßnahme angesehen werden kann. Je höher die Wirksamkeit einer Maßnahme, desto umfangreicher werden potentielle Fehler erkannt. An dieser Stelle wird nun der Vorteil der vorgestellten Vorgehensweise deutlich: Man kann einen direkten Zusammenhang zwischen dem Schweregrad eines Schadens und den geeigneten risikomindernden Maßnahmen erkennen [Tab. 3]. Auf Grundlage dieses Postulats ist in Tab. 2 auch erkennbar, dass eine zweikanalige Architektur („überwachte Redundanz“) eher für Ausfälle in Frage kommt, die einen hohen Schweregrad eines Schadens nach sich ziehen. Für Ausfälle mit weniger gravie-

anzunehmende Fehlerursachen	risikomindernde Maßnahmen		
	überwachte Redundanz (Zweikanaligkeit)	Überwachung während des Betriebs	Hardware mit automatischen Tests
stuck-at	✔	✔	✔
Unterbrechung	✔	✔	✔
Kurzschlüsse	✔	✔	✔
Drift	✔	✘	✔
Oszillation	✔	✘	✔

Tab. 4: Beispiele für die Wirksamkeit von alternativen Maßnahmen. Die Wirksamkeit ist abhängig von der detaillierten applikationsspezifischen Umsetzung der jeweiligen Maßnahme!

renden Auswirkungen stellt die Zweikanaligkeit eine eher überdimensionierte Maßnahme dar. Sicherlich eine zu diskutierende Behauptung, zumal im Anhang ZA der EN ISO 14971 klargestellt wird, dass ökonomische Betrachtungen bei der Risikominderung keine Rolle spielen dürfen und Risiken so weit wie möglich reduziert werden müssen. Wenn die inhärente Sicherheit allerdings schon mit einfachen technischen Mitteln erreicht werden kann, wird sich das Risiko mit aufwendigeren oder zusätzlichen Maßnahmen auch nicht mehr weiter senken lassen.

Anhand einiger Beispiele werden die oben aufgeführten Aspekte sicherlich etwas transparenter. In Medizinprodukten wird die Sensorik oft zweikanalig ausgelegt. Ziel ist es dabei zwei unabhängige Messwerte zu erhalten, diese zu vergleichen und bei unterschiedlichen Werten auf einen Fehler in einem der Sensoren zu schließen. Im Falle einer einkanaligen Auslegung müsste man Fehler mit alternativen risikomindernden Maßnahmen aufdecken. Orientiert man sich dabei an der Tab.1 der EN 61508-2, sollte für jeden potentiellen Fehler eine entsprechende Maßnahme gefunden werden, um diesen aufzudecken. „Überwachung während des Betriebs“ und „Analogsignal-Überwachung“ sind Maßnahmen, die man auch mit dem Überbegriff Plausibilitätsabfragen deklarieren kann. Diese sind häufig ein bewährtes Mittel, um Unterbrechungen, Kurzschlüsse oder auch stuck-at-Fehler aufzudecken [Tab. 4]. Sobald das Signal nicht mehr einem definierten Erwartungswert entspricht, kann man auf einen Fehler schließen. Eine Voraussetzung für die Wirksamkeit der Maßnahme wäre allerdings, dass das Sensorsignal dynamisch ist, sich also stetig verändert. Liegen in einer Applikation dahingegen statische Signale vor, wären eher „Hardware mit automatischen Tests“ oder „Testmuster“ die geeigneten Maßnahmen. In diesem Fall werden zyklisch Testsignale oder Testmuster auf das Nutzsignal oder direkt auf den Sensor gegeben, um festzustellen, ob die Sensorik noch in der Lage ist, die Signalpegel richtig darzustellen und auszuwerten. Je nach Applikation und Umsetzung dieser Maßnahme ist es sogar möglich, die weiteren anzunehmenden Fehlerursachen Drift und Oszillation aufzudecken, indem man beispielsweise ein Referenzobjekt zyklisch von der einkanaligen Sensorik vermessen lässt. Bei optischen Sensoren könnte das ein Testbild sein, bei Drucksensoren eine Referenzmessung, gegebenenfalls im Ruhezustand vor jeder Anwendung. Für die Erkennung von Drift und Oszillation ist auch ein „Referenzsensor“ eine adäquate Maßnahme mit hoher Wirksamkeit, die allerdings auch wieder als eine Variante einer zweikanaligen Architektur anzusehen ist und man möglicherweise vermeiden möchte.



Tab. 5: Risikomanagement mit Unterstützung der EN 61508-2

Auf ähnliche Weise kann man im Risikomanagement Schritt für Schritt weitere Komponenten und Funktionsblöcke eines Medizinproduktes bearbeiten [Tab. 5]. In der zweiten Spalte der Tabellen in Tab. 2 sind Verweise auf entsprechende Kapitel der EN 61508-7 aufgeführt, in der die einzelnen Verfahren zur Risikominderung noch detaillierter beschrieben sind, wodurch man nützliche Hinweise für die praktische Umsetzung erhält.

Eine zweikanalige Architektur ist bei einer Sensorik sicherlich eine einfache Methode, um die Erstfehlersicherheit zu gewährleisten und erfordert relativ wenig Entwicklungsaufwand. Wer allerdings eine zentrale Controllereinheit zweikanalig aufsetzen möchte, steht vor einer großen Herausforderung und ist für die vorgestellte alternative Vorgehensweise sicherlich dankbar. Diese erfordert zwar eine vergleichbare Sorgfalt bei der Ausarbeitung, kann sich jedoch bei den Material- und Herstellkosten langfristig positiv auswirken. Dies ist im Einzelfall sicherlich kritisch zu betrachten. Festzuhalten aber bleibt, dass ein einkanaliges System mit entsprechenden Maßnahmen durchaus mit einer zweikanaligen Architektur konkurrieren und eine vergleichbare Wirksamkeit bezüglich der Risikominderung herbeiführen kann. Eine in der Regel geringere Systemkomplexität ist meist noch ein positiver Nebeneffekt, da jede zusätzliche Komponente – und das kann auch ein zweiter Kanal sein – zusätzliche Fehlerursachen und Risiken mit sich bringen kann, die es zu vermeiden gilt.

Kontakt

embeX GmbH
Heinrich-von-Stephan-Straße 23
79100 Freiburg
www.embex.de

Autor Jochen Metzger
Leiter des Geschäftsbereichs Medical Engineering bei embex