Funktionale Sicherheit bei Medizinprodukten

Medizinische elektrische Geräte müssen so entwickelt und hergestellt werden, dass sie erstfehlersicher oder risikofrei in der Anwendung sind. Um dies nachhaltig zu erreichen, leisten Sicherheitsnormen entsprechende Hilfestellung. Sie geben außerdem Einblick in den neuesten Stand der Technik

Autor | **Jochen Metzger**

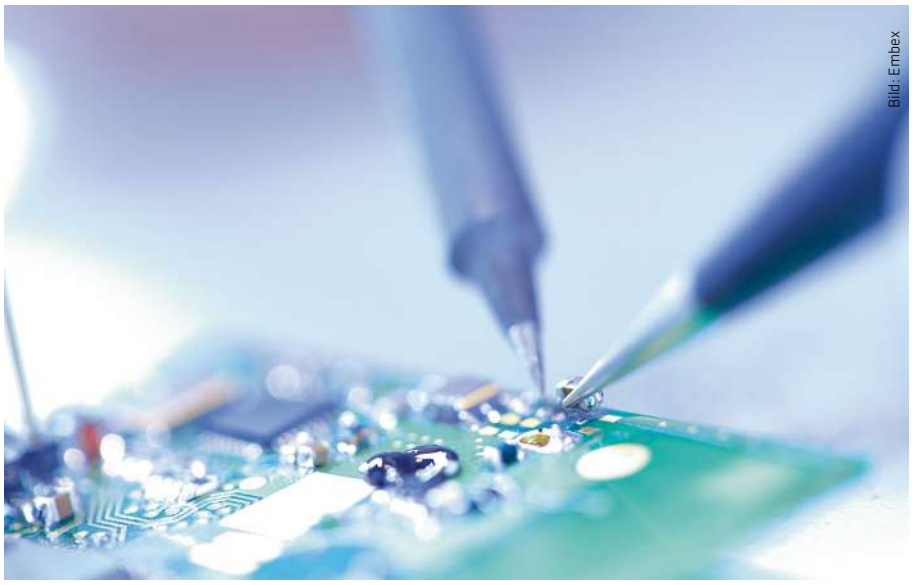

Bild 1 | Sicherheitsnormen: Ziel für Medizintechnikhersteller muss stets sein, Erstfehlersicherheit zu erreichen. Das stellt hohe Anforderungen an den Entwicklungsprozess, insbesondere bei der Auswahl von Verfahren und Maßnahmen zur Risikominderung

Die IEC 61508 ist eine Sicherheitsgrundnorm, aus der weitere anwendungsspezifische Normen abgeleitet werden. Darunter fallen die IEC 61511 (Prozessindustrie) und die IEC 62061 (Maschinensicherheit), allerdings nicht, wie oft behauptet, die IEC 60601.

Sicherheit in vier Stufen

Sicherheitssysteme werden in der IEC 61508 in vier diskrete Stufen eingeteilt, wobei der Sicherheits-Integritätslevel (SIL) 1 die niedrigste, der Sicherheits-Integritätslevel 4 die höchste Stufe darstellt. Je höher der Sicherheits-Integritätslevel, desto geringer muss die Wahrscheinlichkeit eines gefahrbringenden Ausfalls des Systems sein. Es stellt sich die Frage, wie eine Verbindung zwischen dem Sicherheits-Integritätslevel der IEC 61508 und einer Risikoklassifizierung von Medizinprodukten hergestellt werden kann.

Hier bietet sich die IEC 62304 an, deren Anhang C die IEC 61508 als mögliche Quelle für „gute Software-Methoden, -Techniken und -Werkzeuge“ nennt. Die IEC 62304 stellt einerseits Forderungen an den Software-Lebenszyklus-Prozess, enthält aber auch eine Sicherheitsklassifizierung in Abhängigkeit der Auswirkungen auf die Gefährdung von Personen.

Gefahren vermeiden

Auch der Sicherheits-Integritätslevel gemäß IEC 61508 wird auf Grundlage eines Risikographen ermittelt, in dem das Schadensausmaß auf Personen einer der entscheidenden Parameter ist. Ein Beispiel ist im Teil 5 der aus sieben Teilen bestehenden Norm erläutert. Weitere Parameter sind die Auftretenswahrscheinlichkeit eines gefährlichen Vorfalls, die Häufigkeit und Aufenthaltsdauer im gefährlichen Bereich sowie die Möglichkeit, den gefährlichen Vorfall zu vermeiden. Die Betrachtung dieser Parameter findet sich bei einem Medizinprodukt in der Regel in der Risikoabschätzung der Gefährdungssituationen nach ISO 14971 wieder.

Stellt man den Risikographen der IEC 61508 den Medizinprodukteanforderungen und -randbedingungen gegenüber, ergeben sich für viele oder sogar die meisten (programmierbaren) elektrischen Medizinprodukte bzw. -systeme Sicherheits-Integritätslevel von SIL 2 oder SIL 3. Die erforderlichen Maßnahmen zum Vermeiden und Beherrschen von Ausfällen während des Betriebs können nun aus den jeweiligen Anhängen A und B der IEC

61508-2 und IEC 61508-3 ausgewählt werden, die sich in erster Linie auf Hard- und Software sowie den Entwicklungsprozess, aber auch andere Lebenszyklusphasen beziehen.

Wirksamkeit der Verfahren

Je höher der Sicherheits-Integritätslevel definiert wird, desto höher muss auch die Wirksamkeit sein, gefahrbringende Fehler zu erkennen. In den Anhängen A und B der IEC 61508-2 sind beispielhaft Maßnahmen zur Beherrschung von zufälligen Hardware-Fehlern mit der Einstufung niedriger, mittlerer und hoher Wirksamkeit aufgeführt. Ausgehend von einem zuvor definierten Sicherheits-Integritätslevel SIL 2 oder SIL 3 für ein Medizinprodukt kann man als groben Anhaltspunkt festhalten, dass Systeme mit 1-kanaliger Architektur Sicherheitsmaßnahmen mit mittlerer bis hoher, 2-kanalige Systeme Maßnahmen mit niedriger bis mittlerer Wirksamkeit erfordern. Verfahren und Maßnahmen für sicherheitsbezogene Software können für die jeweiligen Sicherheits-Integritätslevel direkt aus den Tabellen in den Anhängen A und B der IEC 61508-3 abgeleitet werden.

Es ist zu beachten, dass nicht der definierte Sicherheits-Integritätslevel, sondern immer die für das Medizinprodukt durchzuführende Risikoanalyse maßgebend für die Auswahl der erforderlichen und risikomindernden Sicherheitsmaßnahmen ist. Nur so erreicht man die erforderliche Integrität des Sicherheitssystems. Wer mit der IEC 61508 nicht vertraut ist, wird sich aufgrund des Umfangs der Norm anfangs etwas schwer tun, die essentiellen Informationen herauszuziehen. Es sind jedoch nur jeweils die Anhänge A und B der IEC 61508-2 und der IEC 61508-3, die die entsprechenden Vorschläge und Empfehlungen zu Sicherheitsmaßnahmen enthalten, so dass nach einer kurzen Orientierungsphase die Anwendung gelingen dürfte. Detaillierte Beschreibungen zur Umsetzung der Verfahren und Maßnahmen finden sich außerdem in der IEC 61508-7.

Der dargestellte Ansatz stellt eine hilfreiche Verbindung zwischen der grundlegenden Sicherheitsnorm IEC 61508 und den Medizinprodukte-Normen her und erleichtert damit die Auswahl geeigneter Sicherheitsmaßnahmen auch im Hinblick auf den derzeitigen Stand der Technik zusehends. Hierbei ist allerdings zu beachten, dass die IEC 61508 ihren Ursprung in der Prozessindustrie und Automatisierungstechnik hat und die sich daraus ergebenden Fragestellungen nicht immer mit denen von Medizinprodukten decken. Die normative Anwendung der IEC 61508 auf medizinische Produkte und Systeme ist daher bewusst ausgeschlossen, eine Anwendung kann somit nur auf informativer Ebene erfolgen.

Sicherheit geht vor

Medizinische elektrische Geräte müssen gemäß IEC 60601-1 so entwickelt und hergestellt werden, dass sie erstfehlersicher sind oder dass das mit der Anwendung verbundene Risiko vertretbar ist. Die einschlägigen Medizinproduktenormen geben allerdings kaum Hinweise, wie diese Erstfehlersicherheit erreicht werden kann. Als Hilfestellung kann hier die als Stand der Technik bewährte Sicherheitsgrundnorm IEC 61508 „Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme“ herangezogen werden.

» **Jochen Metzger,**
Leiter BU Medical Engineering
Embex GmbH
D-79115 Freiburg,
www.embex.de