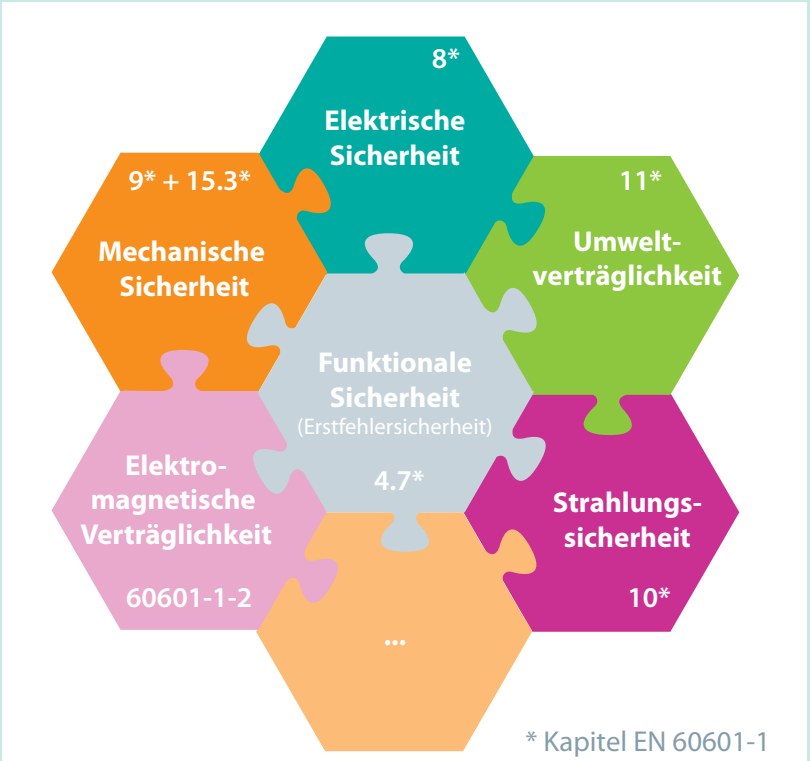
Die Erstfehlersicherheit von Medizinprodukten muss unbedingt gewährleistet sein. Aber wie kommt man ohne Umwege zu diesem Ziel?

Von der Risikoanalyse zum Sicherheitskonzept

Die Gesamtsicherheit eines elektrischen Medizinprodukts setzt sich aus einzelnen Sicherheitsaspekten zusammen (**Bild 1**). Ein Teil stellt die funktionale Sicherheit dar, von der die korrekte Funktion eines Produkts oder Systems abhängt. Im Zusammenhang mit Medizinprodukten spricht man auch von der Erstfehlersicherheit, deren Anforderungen aus der Normenreihe EN 60601 resultieren und deren Erlangung immer in Verbindung mit der Anwendung eines Risikomanagementprozesses nach EN ISO 14971 steht.

Leider ist es immer noch weit verbreitet, altbewährte Sicherheitsmaßnahmen wie Redundanz und Diagnosen unstrukturiert anzuhäufen in der Hoffnung, so ein funktional sicheres Produkt entwickeln zu können. Oft steht das finale Sicherheitskonzept schon, bevor es einen ersten Entwurf für die Risikoanalyse gibt. Nach dem Motto ›Viel hilft viel‹ schießt man möglicherweise mit Kanonen auf Spatzen. Die Sicherheitsintegrität ist mitunter genauso wenig gewährleistet wie bei einem System, bei dem die Sicherheitsmaßnahmen grundsätzlich vernachlässigt wurden. Alles andere wäre purer Zufall. Höhere Herstellungskosten sind das geringere Übel bei dieser Vorgehensweise, Verletzungen oder der Tod von Menschen sind Folgen, die es selbstredend zu verhindern gilt.

Das Risikomanagement erfolgt meist mithilfe von Tabellenkalkulationsprogrammen, Datenbanken oder auch mit kommerziell erhältlichen Tools. Der Fokus liegt dabei auf der Risikoanalyse und der Risikobewertung. Es werden zwar



1 Abgrenzung verschiedener Sicherheitsaspekte

Bildquellen: embeX GmbH

Kontakt

embeX GmbH
D-79112 Freiburg
Tel. +49 (0)761 4797990
Fax +49 (0)761 479799-99
www.embex.de

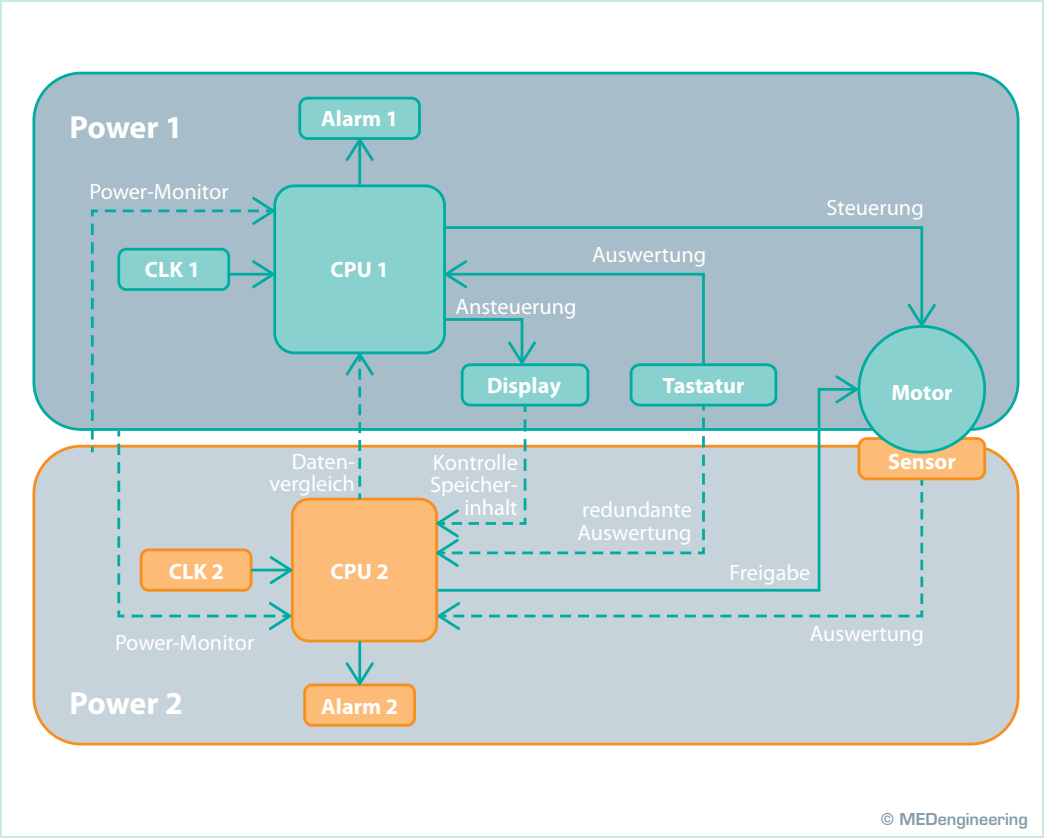
risikomindernde Maßnahmen ausgewählt und die Risikominderung entsprechend bewertet, eine zusammenhängende Darstellung des Sicherheitskonzepts oder der Sicherheitsarchitektur bleibt aber meist schon aus Gründen der eingeschränkten Darstellungsmöglichkeiten der verwendeten Hilfsmittel außen vor. Eine zusammenfassende und übersichtliche Dokumentation eines Sicherheitskonzepts erlaubt es jedoch dem Projektteam, sich mit den einzelnen ausgewählten Sicherheitsmaßnahmen auseinanderzusetzen, deren Zusammenspiel zu analysieren und schlussendlich ein integres Konzept zu erarbeiten. Das Sicherheitskonzept bietet darüber hinaus auch neuen Projektmitgliedern oder Außenstehenden, beispielsweise Projektpartnern oder Prüfbehörden, einen schnellen Einstieg in die wichtige Thematik, ohne umfangreiche Spezifikationen sichten zu müssen. Das Vorhandensein eines Sicherheitskonzepts oder einer Sicherheitsarchitektur als eigenständiges Dokument ist nicht zwingend vorgeschrieben, hat sich jedoch aufgrund der auf der Hand liegenden Vorteile als nützlich erwiesen. Wie bringt man nun eine Struktur in die Erarbeitung eines schlüssigen Sicherheitskonzepts?

Schneller Einblick für Externe

Ausgehend von einem zwingend vorgeschriebenen Risikomanagement nach EN ISO 14971 kann man voraussetzen, dass mögliche Gefährdungen, die aus der Anwendung eines Medizinprodukts resultieren, in der Risikoanalyse vollständig erfasst wurden. Hierbei sind auch die Anforderungen zur Erstfehlersicherheit aus der EN 60601-1 und deren Ergänzungs- sowie Partikularnormen zu berücksichtigen. Nach der Dokumentation und Bewertung möglicher Fehlerquellen sowie Auftretens- und Entdeckungswahrscheinlichkeiten folgt im nächsten Schritt die Auswahl der entsprechenden risikomindernden Maßnahmen.

Das ist auch schon der entscheidende Punkt. Sicherheitsmaßnahmen sind nur dort zwingend erforderlich, wo ein Risiko besteht, wobei das Risiko die Kombination aus Auftretenswahrscheinlichkeit und Schweregrads eines Schadens darstellt. Da man in der Risikoanalyse die Betrachtung der Gefährdungen in der Regel in Bezug auf einzelne Funktionalitäten oder Baugruppen des Produkts untergliedert, wählt man die risikomindernden Maßnahmen meist auch punktuell aus. An dieser Stelle kommt das Sicherheitskonzept ins Spiel: Nicht nur die rein funktionale Hardware oder Software eines Produkts muss im Hinblick auf einen korrekten Betrieb aufeinander abgestimmt werden. Auch die ausgewählten Sicherheitsmaßnahmen müssen miteinander harmonieren, sodass in einer Sicherheitskette keine Lücken entstehen. Was nützt beispielsweise »

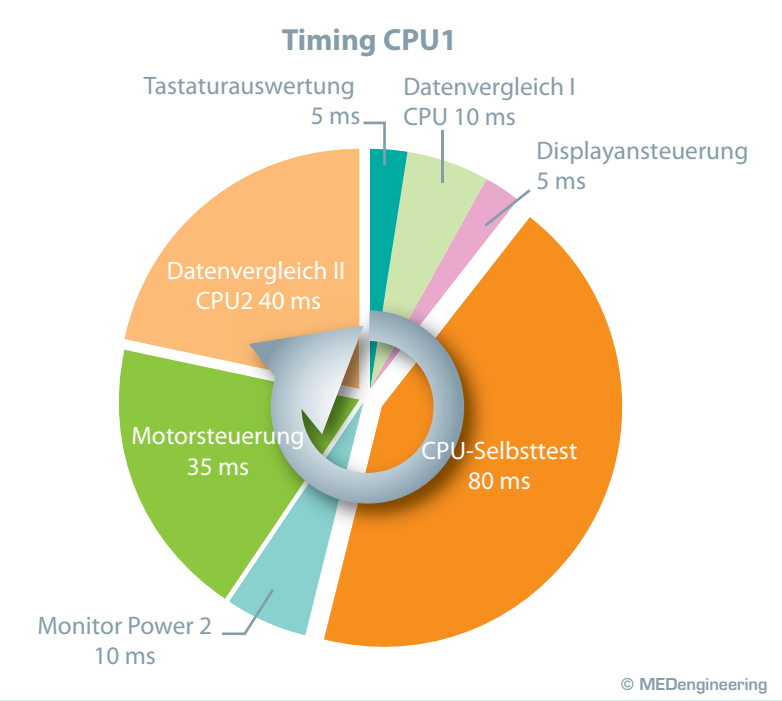
Lückenlose Sicherheit



2 Beispiel für eine Hardware-Architektur

» ein abgesichertes Kommunikationsprotokoll, wenn bei einem einzelnen Kommunikationsteilnehmer die lokale Datenintegrität im Speicher nicht gegeben ist.

Man kann nun auf zwei Wegen einen Einstieg in ein Sicherheitskonzept finden. Entweder man wählt zunächst für jedes in der Risikoanalyse herausgearbeitete Risiko eine risikomindernde Maßnahme punktuell aus und verknüpft alle Sicherheitsmaßnahmen zu einem ersten Entwurf eines Sicherheitskonzepts, oder man beginnt mit einer groben Sicherheitsarchitektur und prüft dann, ob alle Risiken aus der Risikoanalyse abgedeckt sind. Egal welchen Weg man wählt, es wird immer ein iterativer Prozess sein, bis dieser Teil des Risikomanagements sorgfältig ausgearbeitet wurde und schlussendlich ein integres Sicherheitskonzept gegeben ist.



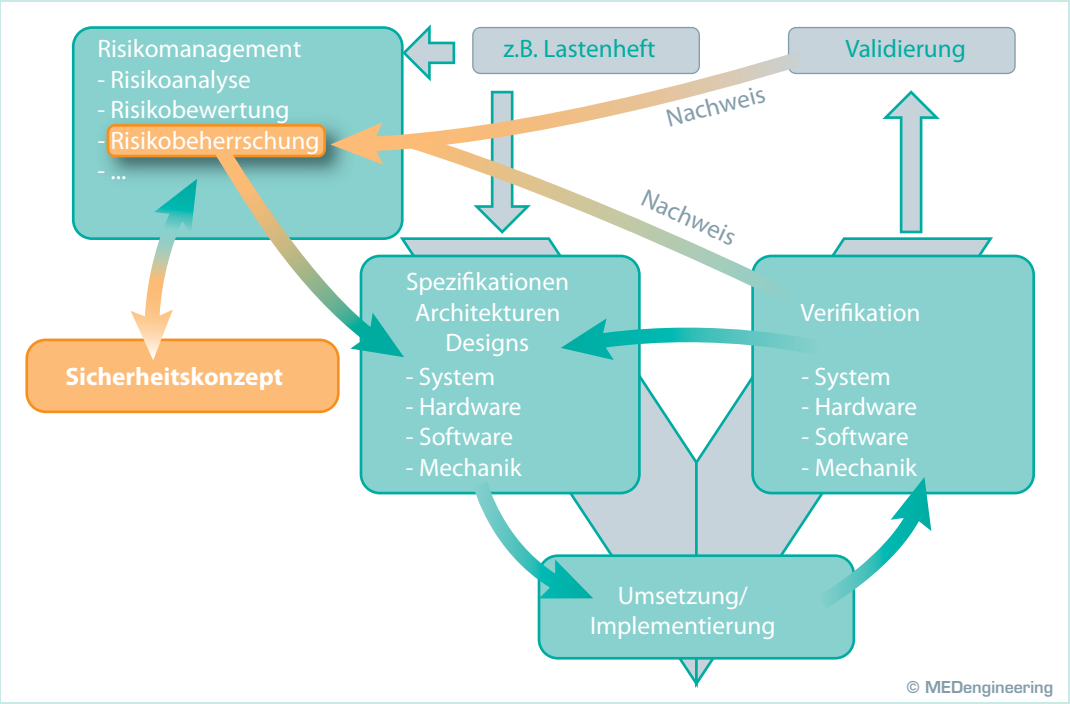
3 **Beispiel für ein CPU-Timing**

Bei dieser Vorgehensweise wird ein relevanter Unterschied deutlich: Während in der Risikoanalyse die risikomindernden Maßnahmen oft nur aufgelistet sind, bietet das Sicherheitskonzept eine zusammenhängende Darstellung und Beschreibung der Sicherheitsarchitektur. Neben den bereits zuvor aufgeführten Vorteilen werden darüber hinaus auch die Lesbarkeit und die Verständlichkeit erhöht. Je nach Detaillierungsgrad des Sicherheitskonzepts wird man feststellen, dass manche Maßnahmen aus technischen Gründen nicht umsetzbar sind und alternative Wege zur Risikominderung gefunden werden müssen. Mit der konzeptionellen Ausarbeitung erhält man mitunter auch eine Verifizierung der Machbarkeit, wodurch das Projektrisiko gemindert wird.

In der EN 61508 (jeweils in den Anhängen A und B der Teilnormen 2 und 3) findet man übrigens zu einzelnen Fehlerquellen sehr gute Ansätze und Alternativen für passende Sicherheitsmaßnahmen, die weitgehend dem Stand der Technik entsprechen. Mithilfe dieser Norm lassen sich in Abhängigkeit der Risiken recht einfach mehr oder weniger wirksame Verfahren auswählen. Je höher das Risiko, desto höher sollte in diesem Fall die Wirksamkeit der Sicherheitsmaßnahme beziehungsweise die Aufdeckungswahrscheinlichkeit eines Fehlers sein. Bei der Gestaltung des Sicherheitskonzepts kann man sich an der reinen Funktionalität des Medizinprodukts orientieren. So wie die einzelnen Baugruppen und Funktiona-

Sicherheitskonzept Kommunikationsprotokoll		Sicherheitsmaßnahmen			
		Datensicherung	laufende Nummer	Zeiterwartung	Authentizität
Fehlermöglichkeiten	Verfälschung	X			
	Wiederholung		**X**		
	Abfolge		X		
	Verlust		X		
	Verzögerung			X	
	Einfügung		X		X
	Maskerade				X
	Adressierung				X

4 **Darstellungsbeispiel für die Absicherung eines Kommunikationsprotokolls**



5 Eingliederung des Sicherheitskonzepts in einen Entwicklungsprozess

litäten zusammenspielen, müssen auch die Sicherheitsmaßnahmen aufeinander abgestimmt sein. Anstatt in ausschweifender Prosa die Sicherheitsmaßnahmen zu beschreiben, können Skizzen, Tabellen oder Diagramme zum besseren Verständnis beitragen. Wie so oft, gilt auch hier: Bilder sagen mehr als tausend Worte. Für die Hardwarearchitektur bietet sich beispielsweise eine Skizzierung auf Blockschaltbildebene an, aus der das Zusammenspiel der einzelnen Baugruppen und die entsprechenden Sicherheitsmaßnahmen wie Redundanzen und Diagnosen hervorgehen (**Bild 2**). Die einzelnen Blöcke können nochmals in gesonderten Blockschaltbildern funktional vertieft werden. Für das Timing kann ein Diagramm (**Bild 3**), für die Absicherung eines Kommunikationsprotokolls hingegen eine Tabelle (**Bild 4**) eine sinnvolle Darstellung sein.

Übersichtliche Darstellung

Kurze Beschreibungen zu den Darstellungen reichen aus, um dem Betrachter das Gesamtkonzept nahezubringen. Die bei der Risikominderung ausgewählten Sicherheitsmaßnahmen können als zusätzliche Anforderungen in entsprechende Spezifikationen mit aufgenommen und dort in angemessener Detailtiefe spezifiziert werden, damit einerseits dem Entwicklungsteam die Umsetzung in Hardware, Software oder Mechanik gelingt und andererseits über den Verifikations- und Validierungspfad der Nachweis für die Wirksamkeit der ausgewählten Maßnahmen erfolgen kann (**Bild 5**). Dabei ist es obligatorisch, in den Spezifikationen die Herkunft der einzelnen Anforderungen mit einem Verweis auf die Risikoanalyse jeweils mit entsprechender Identifikation der risikomindernden Maßnahme zu kennzeichnen, um die geforderte Rückverfolgbarkeit zu gewährleisten.

Es reicht im Übrigen nicht aus, das nach EN ISO 14971 geforderte Risikomanagement nur zu Beginn einer Produktentwicklung anzuwenden. Neben der kontinuierlichen Anwendung des Risikomanagements während des gesamten Produktlebenszyklus ist es auch im Laufe einer Entwicklung zwingend erforderlich, die bestehende Risikoanalyse regelmäßig zu hinterfragen und zu prüfen, ob man einzelne Risiken neu bewerten muss oder ob neue Gefährdungen oder Fehlerursachen hinzugekommen sind. Schließlich erhöht sich mit jeder zusätzlichen Sicherheitsmaßnahme die Komplexität eines Produkts, was durchaus zu neuen Fehlerursachen und Risiken führen kann, die wiederum weitere risikomindernde Maßnahmen und somit eine Überarbeitung des Sicherheitskonzepts nach sich ziehen können. Daraus resultiert auch ein wichtiges Ziel eines guten Sicherheitskonzepts: so viel Sicherheitsmaßnahmen wie notwendig, aber so wenig wie möglich. Mit einer strukturierten Vorgehensweise kann dies gelingen.

Jochen Metzger
ist Leiter des Geschäftsbereichs Medical Engineering bei embeX.