Bild: ©ARMMYPICCA - stock.adobe.com

So gelingt die Zulassung medizinischer Geräte

Anforderungs- und risikobasierte Software-Entwicklung hilft nicht nur, Risiken durch Fehlfunktionen oder falsche Handhabung zu reduzieren. Konsequent umgesetzt und entsprechend dokumentiert entspricht sie auch den Anforderungen von Zulassungsbehörden.

Dr. Edgar Gmür, Senior ICT Consultant bei CSA Engineering

Software als Bestandteil der Produkte wird bei der Entwicklung medizinischer Geräte immer wichtiger. Dies bedeutet aber auch eine Zunahme der Komplexität des Systementwurfs, dessen Umsetzung und nicht zuletzt des Aufwandes bei der Zulassung. So wird heute von den Regulationsbehörden erwartet, dass das Design von Hardware und Software aus den Anforderungen und den Risiken systematisch hergeleitet wird und diese Herleitung auch nachvollziehbar ist. Hinzu kommt, dass Normen an Gewicht gewonnen haben. Insbesondere bei Audits und Submissionen wird auf ein normenbasiertes Vorgehen grosser Wert gelegt. Weiter kommt hinzu, dass zur Entwicklung medizinischer Geräte auch bei der Software das Risikomanagement an Bedeutung und Systematik gewonnen hat. Dieser Fachartikel bezieht sich ausschliesslich auf den Software-Teil. Bei der Entwicklung medizinischer Geräte kommt noch eine Reihe anderer Normen hinzu, die beachtet werden müssen.

V-Modell erprobte Vorgehensweise

Um dieser Komplexität möglichst ideal zu entsprechen, bietet sich in der Regel für die Entwicklung medizinischer Geräte das V-Modell (Grafik 1) an. Beim V-Entwicklungsmodell können bereits während der Entwicklungsphase, also schon bei der Definition der Anforderungen und dem Architekturentwurf, die entsprechenden Tests spezifiziert werden. Damit kann unliebsamen Überraschungen entgegengewirkt und unvollständige Systemanforderungen und -spezifikationen können rechtzeitig erkannt werden, da die Testverantwortlichen frühzeitig eingebunden sind.

Anforderungsmanagement

In der Norm ISO/IEC/IEEE 29148 wird die systematische Entwicklung für Software beschrieben. Sie gilt allgemein und hat keinen speziellen medizintechnischen Bezug. Sie

eignet sich deshalb grundsätzlich für das Anforderungsmanagement, denn sie legt Wert auf Charakteristiken für die Erstellung von Anforderungen, dem Requirements Engineering auf System- und Software-Stufe. Es werden folgende Teilprozesse beschrieben:

- Analyse der Stakeholder-Anforderungen
- Analyse der System- und Software-Anforderungen
- Software-Architektur und Detail-Design

Dabei können die einzelnen Teilprozesse iterativ mit einer zunehmenden Verfeinerung durchlaufen werden, wobei die Dekomposition des Systems in die Komponenten die Grundlage bildet. Bei dieser Verfeinerung werden Systemanforderungen und Systemdesign aus den Stakeholder-Anforderungen abgeleitet. Die Hardware- und Software-Anforderungen stellen dann den nächsten Schritt zur Konkretisierung des Systementwurfs dar. Schliesslich sollen mit der Architektur und dem Komponentendesign die Lösung und deren Umsetzung in der Hardware und Software beschrieben werden.

Software-Entwicklung medizinischer Geräte

Die Norm IEC 62304 wiederum beschäftigt sich im Speziellen mit der Entwicklung von medizinischer Software und Software für medizinische Geräte. Hersteller medizinischer Geräte sollten sich deshalb bei den Prozessen, Aktivitäten und Aufgaben auf diese Norm ausrichten. Sie umfasst den gesamten Entwicklungsprozess mit Requirements Engineering, Software-Design, Implementation und Verifikation. Die Norm erwartet von der Architektur eine hierarchische Dekomposition in ein Software-System, Software-Items und Software-Units. IEC 62304 liefert auch Hinweise auf das Risikomanagement. Die Beurteilung der Patienten-Gefährdung bildet einen zentralen Aspekt, wobei je nach Gefährdung drei Stufen definiert sind:

- Stufe A: keine Verletzung oder Schädigung der Gesundheit möglich
- Stufe B: keine schwere Verletzung möglich
- Stufe C: Tod oder schwere Verletzung ist möglich

Die Gefährdung, mögliche Schäden und die daraus abgeleitete Klassifikation sollte idealerweise im Risk Management File dokumentiert werden. An die Klassifikation sind entsprechende Erwartungen hinsichtlich Qualitätsmassnahmen und Dokumentation gekoppelt.

Risikomanagement-Prozess

Neben dem Anforderungsmanagement kommt bei der Entwicklung medizinischer Geräte dem Risikomanagement eine ebenso wichtige Bedeutung zu. Es betrachtet die Gefährdung des Patienten bezüglich gesundheitlichen Schadens – ausgehend von der

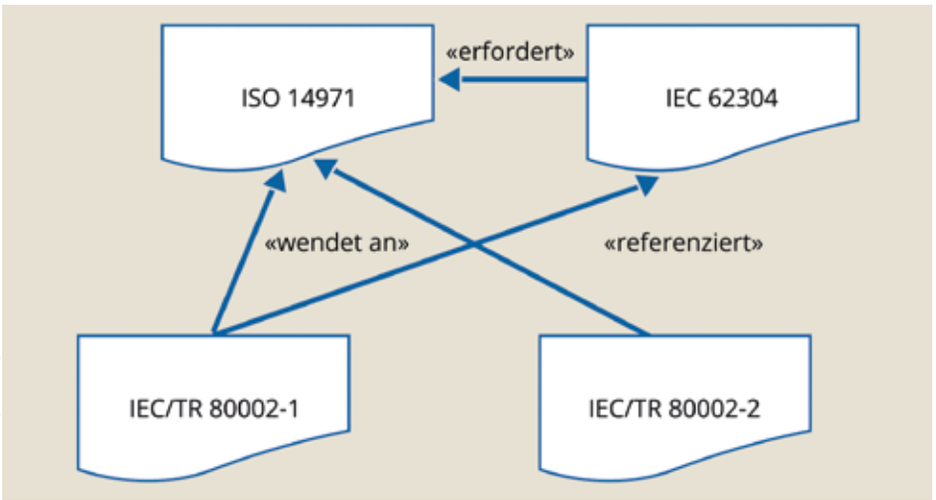

Bild: CSA Engineering

Grafik 2: Risiko- und Anforderungsmanagement: Normen zur Entwicklung medizinischer Geräte.

Software – und vermindert zudem Compliance-Probleme mit den Zulassungsbehörden.

Die U.S. Food and Drug Administration (FDA) beschreibt in ihren Empfehlungen folgende Risikoanalysen:

- «Safety based»-Analyse von Komponenten anderer Hersteller, auch als Software-of-Unknown-Provenance (SOUP) oder Off-the-Shelf (OTS) bezeichnet.
- In allgemeinen Grundsätzen der Software-Validierung werden Aufwände für das Testen und die Validierung der Software in den Kontext des Risikos gestellt.
- Aufwände für Usability Tests, speziell in Bezug auf eine falsche Verwendung des Geräts durch den Benutzer, sollen abhängig vom Risiko sein.
- Die Cybersecurity soll risikobasiert betrachtet werden, besonders wenn ein Gerät mit dem Internet verbunden wird.

Der Software-Entwicklungsprozess und das Risikomanagement stehen bei einer regulatorisch konformen Entwicklung in engem Zusammenhang. Diese Abhängigkeit zeigt sich auch in der Beziehung der Normen untereinander.

Die medizinspezifische ISO-Norm 14971 und die IEC/TR 80002-1/80002-2

Die Norm ISO 14971 beschreibt die Erwartungen für das Risikomanagement bei der Entwicklung eines medizinischen Geräts. Den Kern der Norm bildet ein iteratives Vorgehen – von der Risikoanalyse, der Risikobewertung und der Risikokontrolle mit Definition der Risikominderungsmassnahmen über die Bewertung des Restrisikos nach Anwendung aller Risikomassnahmen bis hin zum Review der Ergebnisse des Risikomanagements. Ergänzend dazu helfen zwei Technical Reports das Risikomanagement von ISO14971 auf die Software anzuwenden. Der erste Report IEC/TR 80002-1 beschreibt die Risikomanagementaktivitäten im Software-Entwicklungsprozess, wohingegen der zweite Report IEC/TR 80002-2 auf die Verifikation der Software eingeht. Für die praktische Umsetzung sind die Tabellen in den Anhängen IEC/TR 80002-1 sehr nützlich. Anhang B.1 liefert eine risikoorientierte Checkliste für das Requirements Engineering und hilft, mögliche Gefährdungen durch die Software frühzeitig zu erkennen. Anhang B.2 wiederum enthält eine Checkliste für das Design und die Programmierung. Hier helfen «Best Practices», den Software-Entwicklungsprozess in Richtung eines sicheren Designs und eines robusten Codes zu steuern. Die Punkte der Checkliste können somit auch als Massnahmen zur Risikominderung betrachtet werden. Für die Umsetzung der Methodik empfiehlt sich, den Anhang B.2 an die verwendete Programmiersprache und Entwicklungsumgebung anzupassen. Einige der Massnahmen können durch automatische Codeanalysen, wie sie z. B. für die Programmiersprache C typisch sind, abgedeckt werden. Andere brauchen eine Überprüfung durch eine oder mehrere Personen und sollten deshalb in den Coding-Richtlinien und in Code-Review-Vorlagen als Checkliste vorgehalten werden.

Dokumentationsprozess

Für die Dokumentation eines medizinischen Geräts werden formale Strukturen im Dokumentationsprozess festgelegt. Anforderungen und Design-Elemente sollen dabei atomar definiert werden und einen festgelegten Satzbau aufweisen. Die Ableitung von Anforderungen und Design-Elementen soll auf der linken Seite des V-Modells von Ebene zu Ebene verlinkt werden. Man spricht hier auch von «Satisfies»-Beziehungen in der Traceability (Nachverfolgbarkeit). Darüber hinaus werden die Anforderungen und Design-Elemente mit den Testfällen auf der rechten Seite des V-Modells verlinkt. Entsprechend spricht man hier von «Validates»-Links in der Traceability. Zudem sollen alle Anforderungen und Design-Elemente auch testbar sein. Falls nötig, können für ein besseres Verständnis die Textbausteine mit festem Satzbau durch weitere Bausteine mit frei formatierten Texten und Diagrammen ergänzt werden. Schliesslich können auch Risiken und Risikoverminderungsmassnahmen aufgenommen werden und mittels einer «Mitigates»-Beziehung mit den Anforderungen und Design-Elementen verlinkt werden. Da bei einem medizinischen Gerät die Anzahl der Textbausteine schnell in die Tausende gehen kann, empfiehlt sich zur Erstellung und Pflege der Textbausteine und der Links der Einsatz von Software-Werkzeugen, wie beispielsweise das Requirements-Management-Tool DOORS von IBM. Mit dem beschriebenen Vorgehen entsteht eine konsistente und nachvollziehbare Dokumentation über alle Disziplinen, Requirements Engineering, Software-Entwicklung, Test-Engineering und Risikomanagement.

Fazit

Mit dem unmittelbaren Einbezug des Risikomanagements in den Software-Entwicklungsprozess kann das Restrisiko für eine Fehlfunktion des Geräts oder eine Gefährdung von Personen infolge falscher Verwendung durch den Patienten massgeblich minimiert werden. Eine konsequente Anwendung eines qualitätsorientierten Entwicklungsprozesses inklusive einer systematischen Dokumentationsmethodik wird deshalb bei Audits und Zulassungen durch Regulationsbehörden eine gute Akzeptanz bewirken.

csa.ch