Sichere Medizingeräte durch strukturierte Sicherheitsnachweise

Strukturierte Sicherheitsnachweise für Medizinprodukte. Jedes Medizinprodukt bringt Gefährdungen für Patienten und Anwender mit sich. Sowohl für die Hersteller als auch für die Zulassungsbehörden und Auditoren stellt sich daher immer die Frage nach der Sicherheit des Produktes. Um diese sicherzustellen, werden Risikoanalysen ausgearbeitet, Maßnahmen definiert und Tests durchgeführt. Dennoch verbleibt am Ende oft noch die Unwägbarkeit, ob wirklich alles Notwendige getan wurde, um bestmögliche Sicherheit zu gewährleisten. Strukturierte Sicherheitsnachweise helfen, diese Unsicherheit zu verringern.

Matthias Hölzer-Klüpfel

■ Alleine in den Jahren 2005 bis 2009 verzeichnete die amerikanische Food and Drug Administration (FDA) mehr als 56.000 Berichte über Probleme mit Infusionspumpen. Probleme, die schwerwiegende Konsequenzen für die Patienten hatten: von simplen Fehlfunktionen (62%) über Verletzungen (34%) bis hin zu Todesfällen (etwa 1%) [1]. Zu den häufigsten Ursachen gehörten Software-Fehler, aber auch Probleme mit der Gebrauchstauglichkeit der Geräte. Viele dieser Fehler erwiesen sich im Nachhinein als absehbar und hätten daher eigentlich im Vorfeld verhindert werden können.

Als Reaktion auf diese Probleme startete die FDA eine Verbesserungsinitiative, die sich direkt an die Hersteller von Infusionspumpen richtet. Diese Initiative besteht aus einer Reihe von Maßnahmen, von denen hier eine besonders betrachtet werden soll: Die FDA verlangt von den Herstellern solcher Infusionspumpen bei der Marktzulassung in Zukunft die Erstellung eines strukturierten Sicherheitsnachweises (safety assurance case). Auch wenn sich diese Forderung im Moment nur auf Infusionspumpen bezieht, so wird es nur eine Frage der Zeit sein, bis diese Form des Nachweises über die Sicherheit von Medizinprodukten auch auf andere Gerätetypen ausgeweitet wird. Denn das Ziel der FDA ist es dabei vor allem, die Prüfung der eingereichten Unterlagen zu verbessern und zu erleichtern.

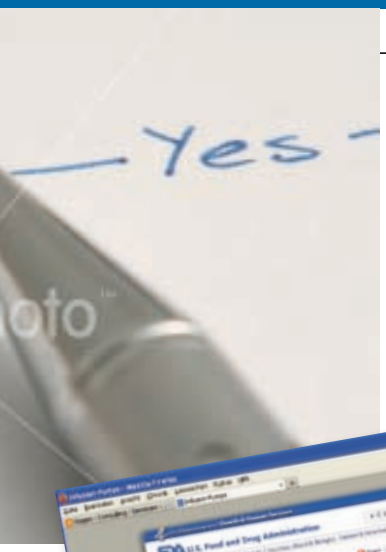
Strukturierte Sicherheitsnachweise

Strukturierte Sicherheitsnachweise zur Beschreibung der Argumentationsketten bei der Beurteilung von Gefährdungen sind kein wirklich neues Werkzeug. In Branchen wie der Kraftwerkstechnik, dem Schiffsbau und in militärischen Anwendungen sind sie schon seit langem im Einsatz. Mit der ISO/IEC 15026-2:2011 [2] steht seit kurzem auch eine Norm zur Verfügung, die die Grundlagen des Vorgehens beschreibt. Das Software Engineering Institute (SEI) der Carnegie Mellon University beschäftigt sich zudem schon seit Jahren mit der Anwendung dieser Methodik auf Medizinprodukte [3].

Bisherige Ansätze, die Sicherheit eines Medizinproduktes nachzuweisen, beruhen meistens darauf festzustellen, dass die eingesetzten Entwicklungsprozesse vorgegebene Standards, wie etwa die ISO 14971 oder die IEC 60601-1, einhalten. Dazu kommt dann noch der Nachweis technischer Prüfungen, die ebenfalls in Produktnormen festgelegt werden. Als problematisch hat sich dabei die Fokussierung auf generelle Prozess- und Produkteigenschaften erwiesen. Denn dabei geraten die Besonderheiten des zu entwickelnden Produktes leicht aus dem Blick. Das Ziel der strukturierten Sicherheitsnachweise ist es nun, anstelle der generischen Prozessanforderungen spezifische Sicherheitsaspekte des jeweiligen Medizinproduktes zu betrachten. Die Grundidee ist, eine schlüssige Argumentation aufzubauen, die Annahmen, Strategien und Belege für die Sicherheit des Gerätes so verknüpft, dass die Grundaussage „Dieses Gerät ist hinreichend sicher“ bewiesen wird. Ein Bild, das in diesem Zusammenhang oft verwendet wird, ist ein Gerichts-

KONTAKT

Method Park Software AG
Wetterkreuz 19a
91058 Erlangen
Tel.: +49 9131 97206-286
Fax: +49 9131 97206-280
E-Mail: email@email.de
www.methodpark.de



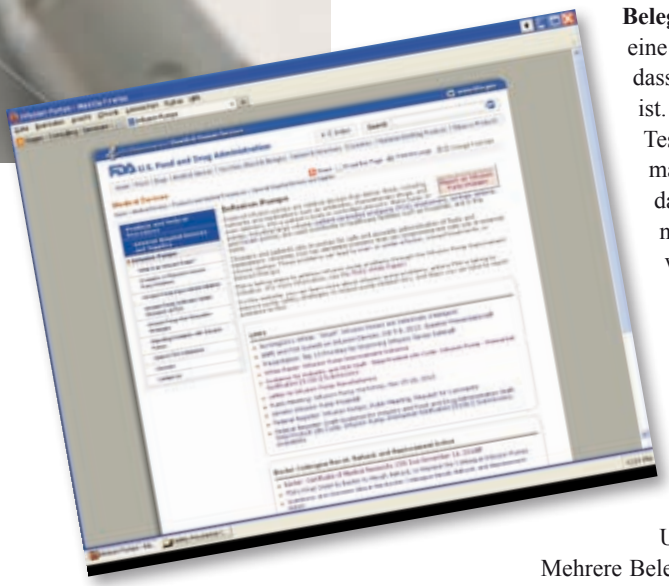


Bild 1: Verbesserungsinitiative der FDA: Verfahrensanweisungen für Hersteller von Infusionspumpen

verfahren, in dem Indizien und Beweise so verknüpft werden, dass die Schuld oder Unschuld eines Angeklagten festgestellt werden kann. Der Sicherheitsnachweis bedient sich dabei der folgenden Konzepte:

Behauptung (claim): Die Behauptung ist eine Aussage, die durch den Sicherheitsnachweis belegt werden soll. Die Behauptungen können hierarchisch strukturiert sein; an oberster Stelle steht dabei immer die These: „Dieses Gerät ist hinreichend sicher."

Strategie (strategy): Die Strategie beschreibt, wie eine Behauptung belegt werden soll. Beispielsweise kann die Strategie darin bestehen, Gefährdungen aufzufinden und sicherzustellen, dass sie eliminiert oder zumindest ausreichend verringert wurden. Eine andere Strategie wäre es, Sicherheitsanforderungen zu identifizieren und zu gewährleisten, dass sie erfüllt wurden.

Annahme (assumption): Eine Annahme beschreibt eine Voraussetzung, unter der die Argumentation gültig ist. Die Annahme unterstützt so Schlussfolgerungen, die unter anderen Umständen eventuell nicht gezogen werden können. Ein Beispiel: Eine Annahme könnte sein, dass ein Fehlverhalten immer dann vorliegt, wenn das Systemverhalten von der Spezifikation abweicht.

Kontext (context): Der Kontext beschreibt zusätzliche Informationen, die für das Verständnis einer Behauptung, Strategie oder eines Beleges notwendig sind.

Wenn eine Behauptung etwa lautet: „Das System erfüllt alle relevanten Normen", dann ist der Kontext dieser Behauptung beispielsweise die Liste der relevanten Normen.

Beleg (evidence): Ein Beleg ist eine Tatsache, die darauf hinweist, dass eine Behauptung korrekt ist. Beispielsweise sind positive Testergebnisse von Sicherheitsmaßnahmen ein Beleg dafür, dass die entsprechenden Maßnahmen erfolgreich umgesetzt wurden.

Der Sicherheitsnachweis ist nun nicht einfach eine lose Ansammlung dieser Elemente, sondern verknüpft sie strukturiert. Eine Behauptung kann sich so etwa auf verschiedene Unterbehauptungen stützen. Mehrere Belege können erst zusammengenommen ausreichen, um etwas zu beweisen. Schlussfolgerungen treffen nur unter einschränkenden Annahmen zu und so weiter. Da diese Zusammenhänge schnell komplex werden, ist es sehr sinnvoll, eine grafische Notation einzusetzen, um die Zusammenhänge anschaulich darzustellen.

Goal Structured Notation

Die „goal structured notation" (GSN) ist eine grafische Beschreibungssprache für Sicherheitsnachweise, die an der Universität von York entwickelt wurde [4]. Sie stellt grafische Elemente für die Konzepte ‚Behauptung', ‚Kontext', ‚Strategie', ‚Beleg' und ‚Annahme' bereit, ebenso für die Beziehungen zwischen diesen Elementen. Bild 2 zeigt diese Elemente in einer Übersicht. Die wesentlichen Strukturelemente (Behauptung, Strategie, Kontext, Belege und Annahmen) wurden im vorangegangenen Abschnitt schon vorgestellt. Die GSN fügt diesen Elementen nun noch eine Reihe von Beziehungen hinzu, mit denen die Elemente verknüpft werden:

gelöst durch (solved by): Die Beziehung ‚gelöst durch' verknüpft die Elemente mit den weiterführenden Elementen, die sie umsetzen.

im Kontext von (in the context of): Die Beziehung ‚im Kontext von' verknüpft eine Behauptung, eine Strategie oder einen Beleg mit dem dazugehörigen Kontext.

benötigt Verfeinerung (requires further development): Die Markierung ‚benötigt Verfeinerung' wird an eine Behauptung angehängt, wenn diese noch nicht vollständig bewiesen wurde. Das Symbol zeigt damit an, dass der Sicherheitsnachweis an dieser Stelle noch nicht vollständig ist.

benötigt Instanziierung (requires instantiation): Diese Markierung wird an einen Beleg angehängt, wenn dieser bisher nur beschrieben wurde, aber noch nicht konkret vorliegt. Ein Beispiel für einen gängigen Beleg sind Testnachweise. Ein Testnachweis wird solange markiert, bis der Test tatsächlich durchgeführt wurde und die entsprechenden Ergebnisse vorhanden sind. Das folgende Beispiel zeigt diese Elemente im Zusammenspiel (Bild 3). Ausgangspunkt ist die Behauptung, das Gerät sei sicher. Die Strategie zum Nachweis dieser Behauptung besteht aus zwei Bestandteilen: Zum einen setzt das Gerät alle Sicherheitsfunktionen, wie sie beispielsweise die einschlägigen Normen fordern, um. Zum anderen werden alle Gefährdungen, die sich etwa aus der Risikoanalyse nach ISO 14971 ergeben, auf ein vertretbares Maß reduziert.

Als Beispiel für einen Funktionsfehler soll eine Überdosierung betrachtet werden. Die Behauptung ist nun, dass eine Überdosierung vom Gerät abgefangen wird. Diese Behauptung soll durch einen Testnachweis sichergestellt werden. Das Beispiel ist natürlich bis dahin nicht vollständig. Die Umsetzung der Sicherheitsfunktionen muss noch nachgewiesen werden, ebenso die Beherrschung der Bedienfehler. Und nicht zuletzt muss schließlich der Testnachweis erbracht werden, der bestätigt, dass eine Überdosis abgefangen wird. Aber der prinzipielle Aufbau eines strukturierten Sicherheitsnachweises lässt sich an dem Beispiel erkennen.

Vorteile der Sicherheitsnachweise

Viele der Informationen, die in einem solchen Sicherheitsnachweis erfasst werden, entstehen auch jetzt schon im Rahmen des Risikomanagements nach ISO 14971. Auf den ersten Blick scheint die strukturierte Darstellung nur eine weitere Dokumentationshürde zu sein. Aber das Konzept des Sicherheitsnachweises bietet auch wertvolle Unterstützung für Hersteller und Auditoren:

Durch den hierarchischen Aufbau werden die Aspekte herausgestellt, die für die Argumentation besonders wichtig sind. In den umfangreichen Tabellen, die üblicherweise bei einer Risikoanalyse entstehen, ist es oft schwieriger, die wichtigsten Punkte klar zu kennzeichnen.

Durch die Verwendung der Markierun-

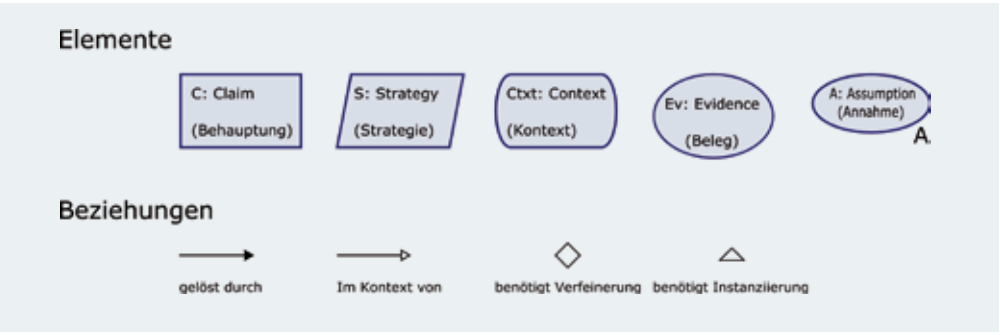


Bild 2: Beschreibungselemente der GSN

gen ‚benötigt Verfeinerung' beziehungsweise ‚benötigt Instanziierung' lassen sich auch Zwischenstände dokumentieren, die vorliegen, wenn die Sicherheitsstrategie noch nicht komplett ausgearbeitet wurde. Das hilft, den Überblick zu behalten und zu garantieren, dass die Sicherheitsbetrachtungen vervollständigt werden.

Mit der einfachen grafischen Notation steht ein gutes Hilfsmittel für die Kommunikation zwischen den am Risikomanagement beteiligten Personen zur Verfügung. Risikomanagement ist ein interdisziplinärer Prozess, und dabei ist es wichtig, die gemachten Überlegungen klar und verständlich festhalten zu können.

Für die Auditoren bietet sich mit einem strukturierten Sicherheitsnachweis die Chance, in der Menge der eingereichten Detailinformationen die wesentlichen Argumente zu erkennen und nachzuvollziehen.

Zusammengenommen lassen diese Argumente den zusätzlichen Aufwand, den die Erstellung eines Sicherheitsnachweises zweifelsfrei mit sich bringt, als angemessen erscheinen.

Erstellung von Sicherheitsnachweisen

Ein Sicherheitsnachweis stellt die Argumente und Belege für die Sicherheit eines Medizinproduktes sehr übersichtlich und nachvollziehbar dar. Dies führt leicht zu der Versuchung, einen solchen Sicherheitsnachweis ans Ende der Entwicklung eines Produktes zu stellen. Denn erst wenn alle Risikoanalysen durchgeführt und alle Tests abgeschlossen sind, stehen die notwendigen Informationen vollständig zur Verfügung. So charmant diese Vorgehensweise erscheint, sie hat einige sehr gravierende Nachteile:

Die Argumentationskette wird ‚von hinten' aufgebaut. Da die Tests und die Ergebnisse der Risikoanalyse feststehen, muss der Sicherheitsnachweis so gestrickt werden, dass diese Ergebnisse ausreichen, um die Behauptung der Sicherheit des Produktes zu belegen.

Viele Argumente, die dazu geführt haben, das Produkt so auszulegen, wie es sich am Ende darstellt, sind eventuell nicht mehr in den Köpfen der Mitarbeiter. Dennoch muss der Sicherheitsnachweis stimmig sein. Dazu müssen unter Umständen die schon einmal durchdachten Schlussfolgerungen neu erarbeitet werden.

Das Design des Produktes ist abgeschlossen; neue Erkenntnisse aus der Erstellung und der Strukturierung des Sicherheitsnachweises lassen sich nicht mehr verwerten.

Sollte sich dabei gar herausstellen, dass die Sicherheit an einigen Stellen nicht ausreichend ist, dann wird ein Redesign des Produktes notwendig. Dies ist mühsam und teuer.

Aus diesen Gründen ist die Empfehlung ganz klar: Der strukturierte Sicherheitsnachweis sollte bereits mit dem Beginn der Entwicklung des Medizinproduktes erstellt und in jeder Phase überarbeitet werden. Er sollte jeweils den aktuellen Stand der Überlegungen hinsichtlich der Sicherheit des Produktes dokumentieren. Wenn dieser Stand für den sicheren Gebrauch am Patienten noch nicht ausreicht, dann bietet der vorläufige Sicherheitsnachweis Anhaltspunkte, um die verbleibenden Lücken zu schließen.

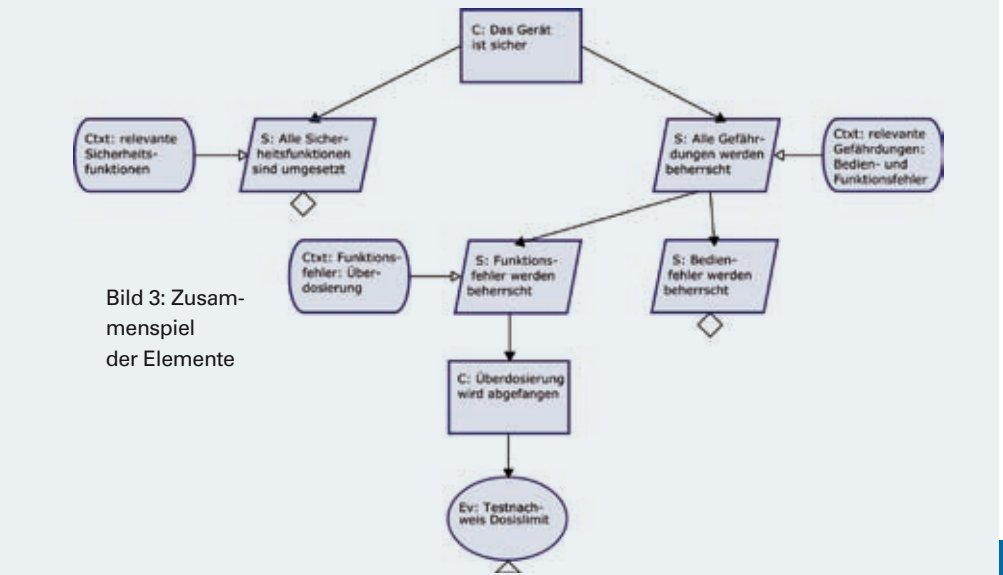


Bild 3: Zusammenspiel der Elemente

Fazit

Auf die Hersteller von Medizinprodukten kommt mit den strukturierten Sicherheitsnachweisen ein neues Instrument zu, das sie in Zukunft beherrschen müssen. Aber der „Safety Case"-Ansatz ist mehr als nur eine weitere Dokumentationshürde. Sinnvoll eingesetzt, lässt sich damit der Prozess des Risikomanagements zielgerichtet gestalten. Denn durch die übersichtliche Darstellung der Argumentation lassen sich die Aufwände bei der Überprüfung der funktionalen Sicherheit auf die wesentlichen Aspekte fokussieren. *wp*

Literatur

[1] Total Product Life Cycle: Infusion Pump — Premarket Notification [510(k)] Submissions; Draft Guidance; U.S. Department of Health and Human Services, Food and Drug Administration, Center for Devices and Radiological Health; 23. April 2010

[2] Systems and software engineering — Systems and software assurance —Part 2: Assurance case; ISO/IEC 15026-2:2011

[3] Ch. Weinstock, J. Goodenough: Towards an Assurance Case Practice for Medical Devices; Technical Note CMU/SEI-2009-TN-018; Software Engineering Institute, Carnegie Mellon University; October 2009

[4] T.P. Kelly: Arguing Safety – A Systematic Approach to Safety Case Management; PhD diss., University of York, Department of Computer Science, 1998

Autor:

Matthias Hölzer-Klüpfel ist als Entwickler, Berater und Projektleiter bei der Method Park Software AG tätig.

www.mechatronik.info

Diesen Artikel finden Sie im Internet, wenn Sie im Feld >Suche< die Dokumentennummer MExxxxxx eingeben.