Beherrschbares Risiko

Sichere Entwicklungsprozesse für Software in der Medizinelektronik definieren und durchsetzen

Mikrocontroller und Industriecomputer übernehmen in modernen Medizinprodukten zunehmend Aufgaben, für die zuvor elektrische oder mechanische Komponenten zuständig waren. Die Qualität der eingesetzten Software erhält bei der Medizinelektronik besondere Brisanz – klar dass hier der Gesetzgeber regulierend eingreift.

Autor: Matthias Hölzer-Klüpfel

Viele moderne Medizinprodukte sind komplexe Systeme, bestehend aus mechanischen, optischen und elektronischen Komponenten. Da sie für die diagnostische oder therapeutische Anwendung am Menschen vorgesehen sind, gefährden sie unweigerlich die Patienten und die Bediener. Diese Gefahren so weit zu reduzieren, dass der medizinische Nutzen das Risiko übersteigt, ist eines der zentralen Anliegen der gesetzlichen Regelungen, die für Medizingeräte gelten. Leider sind diese Regelungen weder einfach noch einheitlich, so dass sich die Entwickler intensiv mit der Compliance ihrer Produkte auseinandersetzen müssen.

Rechtlicher Rahmen

Die gesetzlichen Regelungen für Medizinprodukte unterscheiden sich von Land zu Land. Schon die beiden größten Märkte für Medizinprodukte, die USA und die EU, gestalten die rechtlichen Rahmenbedingungen sehr unterschiedlich: Während in der EU jeder Hersteller die Verantwortung für die Konformität seiner Produkte mit den gesetzlichen Richtlinien trägt, setzen die USA auf die Überprüfung der Zulassungsdokumente durch die mächtige Bundesbehörde FDA. Allerdings gibt es auch Gemeinsamkeiten: In beiden Fällen bilden internationale Normen und Standards einen wesentlichen Baustein der Anforderungen, welche die Gesetzgeber den Herstellern von Medizinprodukten auferlegen (siehe Infokasten).

Um die Sicherheit von Medizinprodukten zu gewährleisten, reguliert der Gesetzgeber neben vielen technischen Forderungen an die eingesetzten Komponenten auch den Entwicklungsprozess bei der Herstellung von Software. Der Begriff „Software" ist dabei weit gefasst und beinhaltet:

- Software als eingebetteter Bestandteil von Medizinprodukten
- Firmware in Komponenten des Medizinproduktes
- Software als Zubehör zu einem Medizinprodukt
- Software, die ein eigenständiges Medizinprodukt darstellt

Dabei ist es unerheblich, ob ein Hersteller die Software selbst entwickelt, sie sich zuliefern lässt oder indirekt als Teil einer Komponente bezieht. Für das Risiko- und Qualitätsmanagement zeichnet in letzter Konsequenz immer der Hersteller des Medizinprodukts verantwortlich.

„Werkzeuggestützte Prozessmodellierung erleichtert die Entwicklungsarbeit für medizinische Software enorm": Dr. Erich Meier, Vorstand von Method Park in Erlangen

Risiko mit Hard- und Software senken

Zur Anwendung der Norm IEC 62304 (Lebenszyklus, siehe Infokasten) auf medizinelektronische Systeme gehört es unter anderem, Risiken zu beherrschen. Dabei geht die eigentliche Gefährdung nicht direkt von der Software aus; Verletzungen erfordern immer den Kontakt des Patienten mit mechanischen Komponenten. Wenn ein System potenziell solche Gefährdungen aufweist, dann ist der Hersteller in der Pflicht, Maßnahmen zur Reduktion des Risikos einzuleiten. Nachfolgend soll eine Insulinpumpe als Beispiel dienen. Mögliche Gefährdung: das Gerät könnte dem Patienten eine zu hohe Insulindosis verabreichen. Die Ursache dafür kann in der steuernden Software oder in der Mechanik liegen. Beispielsweise könnte die Software eine falsche Dosis berechnen oder die Mechanik gibt, trotz korrekter Berechnung, zu viel Insulin ab.

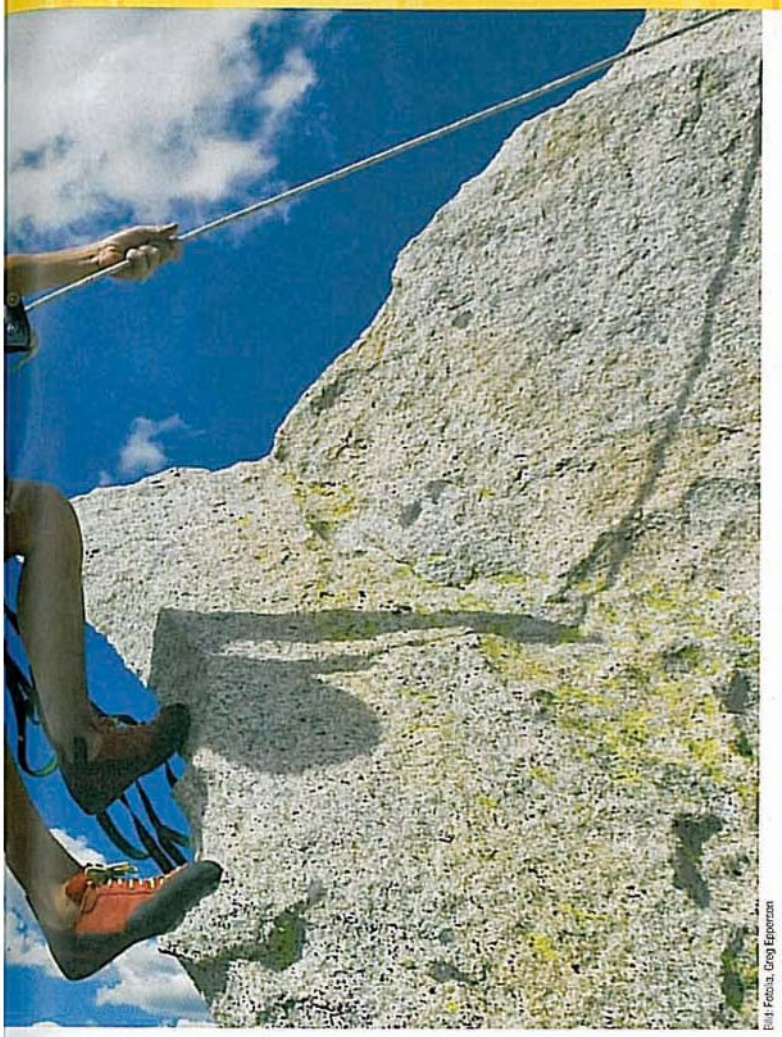


Bild: Fotolia, Greg Epperson

Infokasten

Sicherheitsklassen nach IEC 62304

Die Norm IEC 62304 ordnet Softwarekomponenten eine Sicherheitsklasse zu. Welche Klasse anzusetzen ist, hängt ab vom Ausmaß der möglichen Schädigung durch das Medizinprodukt:

Sicherheitsklasse A: Keine Verletzung oder Schädigung der Gesundheit möglich

Sicherheitsklasse B: Keine schweren Verletzungen möglich

Sicherheitsklasse C: Tod oder schwere Verletzungen möglich

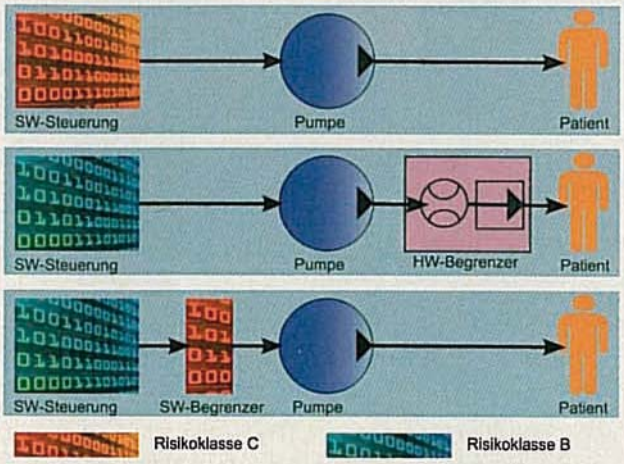


Bild 1: Die Risikoeinstufung der eingebetteten Software kann ein Entwickler reduzieren, indem er zusätzliche Hardware- oder Software-Sicherheitsmaßnahmen vorsieht.

Da eine Überdosis Insulin sogar zum Tod des Patienten führen kann, ordnet die IEC 62304 der Software zur Berechnung der Dosis die höchstmögliche Sicherheitsklasse C zu (siehe Infokasten). Daraus folgen besondere Auflagen an die Vorgehensweise bei der Entwicklung dieser Software.

Aufwand reduzieren

Den Aufwand, den die IEC 62304 vorschreibt, kann man reduzieren, wenn es eine elektronische oder mechanische Schutzvorrichtung gibt, die verhindert, dass das Gerät eine gefährlich hohe Dosis verabreicht. Integriert man beispielsweise einen mechanischen Begrenzer für die Insulinmenge, so kann man die Sicherheitsklasse für die Berechnungssoftware auf B reduzieren.

Die Begrenzung könnte auch durch eine zweite, unabhängige Software erfolgen. Zwar reduziert sich damit die Sicherheitsklasse für die Berechnungssoftware ebenfalls auf B, allerdings erkauft man sich diese durch die neue Begrenzersoftware, die wiederum der Sicherheitsklasse C unterliegt (siehe Bild 1). Oft ist daher ein zusätzliches mechanisches oder elektronisches Element zur Begrenzung des Risikos viel sinnvoller als ein weiteres Stück Software.

Anforderungen an die Entwicklungsprozesse

Während die Entwicklung von mechanischen und elektronischen Systemen meist bewährten ingenieurmäßigen Vorgehensweisen folgt, besteht bei der Gestaltung von Software-Entwicklungsprozessen sehr viel Freiheit. Von strengem, wasserfallartigem Vorgehen bis hin zur agilen Softwareentwicklung findet sich ein weites Spektrum von Modellen.

Die Normen für die Entwicklung medizinischer Software schränken diese Freiheit zwar ein, lassen aber immer noch viel Spielraum für die Kreativität der Entwicklungsabteilungen. Beispielsweise setzt die IEC 62304 einen groben Rahmen für den Ablauf der Softwareentwicklung, des Risikomanagements für Software, des Problemlösungs- und Wartungsprozesses sowie für das Konfigurationsmanagement. Konkrete Vorgaben für die Ausführung einzelner Aufgaben, beispielsweise für den Akzeptanztest von Softwareeinheiten, sieht die Norm aber nicht vor.

Werkzeuggestützte Prozessmodellierung

Die Definition eines Entwicklungsprozesses, der sowohl den normativen Anforderungen genügt, als auch die Freiheit der Entwickler soweit möglich bewahrt, stellt daher eine Herausforderung dar, der sich die Hersteller moderner Medizinelektronik gegenüber →

Auf einen Blick

Prozessordnung

Weil Medizinprodukte direkt am Menschen eingesetzt werden, stellen sie immer eine potenzielle Gefahr dar. Um die Gefährdung gering zu halten, hat der Gesetzgeber den Rahmen eng gesteckt. Sich bei der Softwareentwicklung nötige Freiheiten zu erhalten und gleichzeitig die Vorgaben zu erfüllen, geht am besten mit einem automatischen Werkzeug zur Prozessbeschreibung, das auch beim Abgleich mit den Normen und Standards hilft.

infoDIREKT www.elektronikjournal.de 502ejl7009
Link zu Method Park

VORTEIL Werkzeuggestützte Prozessmodellierung hilft dem Entwicklungsleiter, alle Normen und Vorgaben zu erfüllen, ohne seine Ingenieure unnötig zu gängeln.

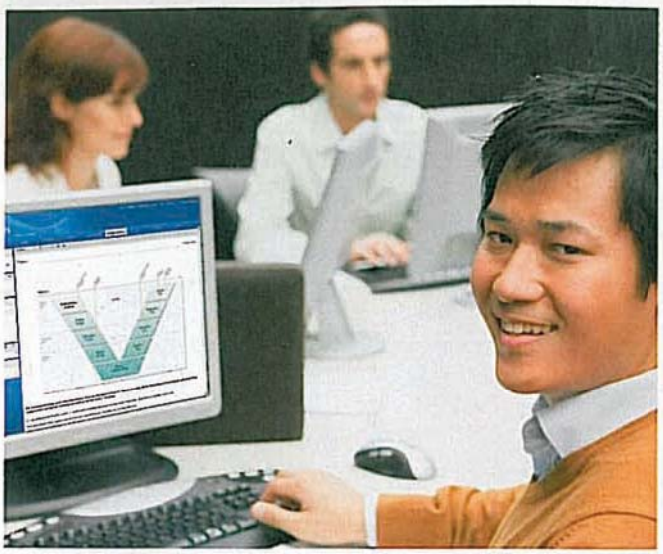
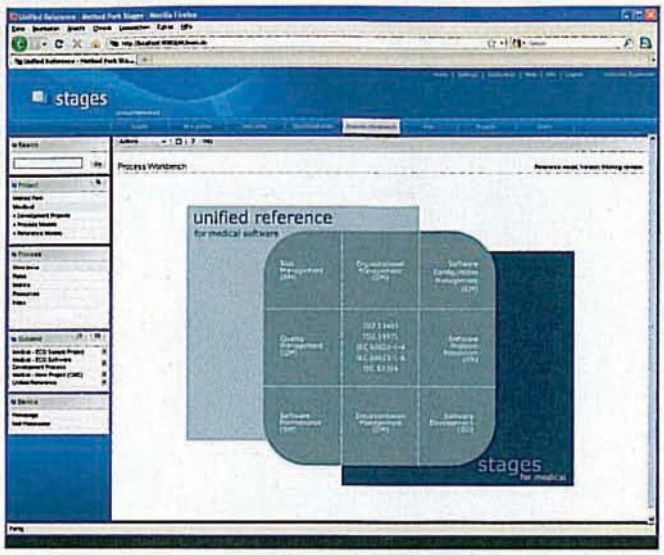


Bild 2: Bei der Softwareentwicklung gibt es eine enorme Vielfalt von Vorgehensmodellen. Die große Herausforderung lautet, einen Entwicklungsprozesses zu definieren, der den normativen Anforderungen genügt und die Entwickler nicht unnötig gängelt.



Abbildungen: Method Park

Bild 3: Stages for Medical modelliert den Entwicklungsprozess so, dass das Management die Abläufe grafisch sieht und die Mitarbeiter jederzeit prüfen können, welche Schritte wann von wem durchgeführt werden müssen. Zudem verifiziert das Tool die Konformität zu den relevanten Normen.

sehen. Prozessmodellierung mithilfe spezieller Entwicklungswerkzeuge bietet eine Möglichkeit, den gesetzlichen Auflagen Rechnung zu tragen und dennoch die größtmögliche Freiheit bei der Prozessgestaltung zu behalten.

Werkzeuge wie „Stages for Medical" der Firma Method Park ermöglichen es dem Entwicklungsteam, ihren Entwicklungsprozess strukturierter zu modellieren und automatisch zu visualisieren. In diesem Schritt entsteht eine konsistente Prozessbeschreibung mit der Definition aller Rollen, Dokumente und auszuführenden Aktivitäten. Im zweiten Schritt wird der Prozess mit den vom Werkzeug bereitgestellten Referenznormen verknüpft. Die harmonisierten Normen der EU sowie die relevanten Gesetze und Guidelines der FDA stehen für diese Verknüpfung zur Verfügung.

Infokasten

Wichtige Normen in der Medizinelektronik

ISO 13485: Eine auf die ISO 9001 abgestimmte, von der EU mit der „Medical Device Directive" harmonisierte Norm, die die Einrichtung eines Qualitätsmanagement-Systems für die Entwicklung und Herstellung von Medizinprodukten beschreibt. Verkürzt kann man sagen: ISO 13485 ist die ISO 9001 für Medizintechnik-Hersteller.

ISO 14971: Diese harmonisierte Norm beschreibt die Anwendung von Risikomanagement auf Medizinprodukte. Risikomanagement bezieht sich in diesem Zusammenhang immer auf Produktrisiken, also auf Gefährdungen, die vom Medizinprodukt ausgehen. Dies muss man klar von den Projektrisiken trennen, also den Gefahren für den erfolgreichen Abschluss beispielsweise einer Produktentwicklung.

IEC 60601-1: Beschreibt die allgemeinen Sicherheitsanforderungen für medizinische elektrische Geräte. Im Kontext von Software sind vor allem die Unternormen 60601-1-4 für programmierbare elektrische medizinische Systeme und die Norm 60601-1-6 zur Gebrauchstauglichkeit relevant.

IEC 62304: Eine Norm für den Lebenszyklus von Software in Medizingeräten beziehungsweise für Medizinprodukte, die nur aus Software bestehen. Die Norm beschreibt Anforderungen an den Prozess der Softwareentwicklung, die von den System-Requirements ausgehend bis zum Test und zur Pflege des Produktes reichen. Besonderes Augenmerk legt die Norm auf die Nachverfolgbarkeit von Anforderungen, die Risikoanalyse der eigenen Software und der Software von Drittherstellern sowie auf die Etablierung von Konfigurations- und Änderungsmanagement.

Abläufe beherrschen

Dr. Erich Meier, Vorstand der Method Park Software AG, führt dazu aus: „Die Beherrschung von Prozessen, also die Steigerung der Produktivität bei gleichzeitiger Konformität zu allen relevanten Regularien, ist eine zunehmende Herausforderung bei der Entwicklung komplexer medizintechnischer Geräte und Systeme. Werkzeuggestützte Prozessmodellierung erleichtert die Entwicklungsarbeit für medizinische Software enorm. Unser Stages for Medical übernimmt das gesamte Prozessmanagement, sichert den Zugriff auf wichtige Dokumente auch über Unternehmensgrenzen hinweg und stellt damit sicher, dass die Entwicklerteams diese Prozesse auch tatsächlich leben."

Die Konformität des Prozesses mit den Normen und Standards lässt sich bei Stages vor Medical werkzeuggestützt verifizieren. Spätere Änderungen am Entwicklungsprozess erhalten auf diese Weise zuverlässig die Konformität. Aber auch die Durchführung der Projekte, die auf dem einmal definierten Entwicklungsprozess basieren, kann jederzeit auf Konformität überprüft werden. Auf diese Weise lassen sich die Akzeptanz der Prozesse erhöhen und Unsicherheiten bei den Zulassungsverfahren verringern.

Qualitätsarbeit

Die Qualität der eingesetzten Software wird auch für moderne Medizinelektronik immer bedeutsamer. Dabei gilt es – nicht nur wegen der gesetzlichen Regelungen – das Augenmerk auf die eingesetzten Entwicklungsprozesse zu richten. Die Kunst ist, die Balance zwischen den normativen Vorgaben und den notwendigen Freiheiten der Entwickler zu finden. Werkzeuge können auch helfen, zu prüfen, ob der eigene Prozess mit den regulatorischen Anforderungen konform geht. *(lei)* ■

Der Autor: Matthias Hölzer-Klüpfel ist Entwickler, Berater und Projektleiter bei Method Park und verantwortet dort den Themenbereich Medizintechnik. Nebenbei schloss er den Masterstudiengang „IT im Gesundheitswesen" ab.