Betriebssysteme stecken in nahezu allen Medizingeräten und müssen den Konformitätsanforderungen ihres Einsatzortes entsprechen. Bei der Zertifizierung gibt es viele Hürden.

OS-Sicherheit für mobile medizinische Geräte

Das Betriebssystem (OS) ist von zentraler Bedeutung für das medizintechnische Gerät: Fällt das OS aus, versagt auch alles andere. Und ein medizintechnisches Gerät ist kein Desktop-PC – selbst bei Geräten der FDA-Klasse I und II sind sporadische Ausfälle und Neustarts inakzeptabel. Als Herzstück eines Rechners stellt es eine Software-Plattform bereit, auf der weitere Applikationen ausgeführt werden können.

Ein OS für ein mobiles Medizingerät muss sich an drei wichtigen Kriterien messen lassen: Verlässlichkeit (das OS reagiert auf Ereignisse korrekt, rechtzeitig und so lange, wie erforderlich), Anbindung (das OS kommuniziert entweder direkt oder über ein Netzwerk mit verschiedenen anderen Geräten und Systemen sowie Datenintegrität und -sicherheit (das OS speichert Daten sicher und schützt sie vor Einsichtnahme durch nicht autorisierte Dritte).

Ein grundlegendes Kriterium bei der Auswahl eines OS ist seine Konformität zu einschlägigen Normen und Bestimmungen und seine Zulassungsfähigkeit in den Märkten, in denen das Medizingerät vertrieben werden soll. In den USA können Medizintechnikhersteller auf zwei Arten eine Marktzulassung erlangen: Für Produkte, die mit bereits von der FDA zugelassenen Produkten vergleichbar sind, kann 90 Tage vor der geplanten Markteinführung ein Antrag auf 510(k)-Zulassung bei der FDA gestellt werden. Andere Geräte müssen zunächst von der FDA geprüft und genehmigt werden, bevor sie auf den Markt gebracht werden dürfen. Darüber hinaus müs-

Kontakt

QNX Software Systems GmbH
D-30177 Hannover
Tel.: 0511 94091-0
Fax: 0511 94091-199
www.qnx.de

sen Medizintechnikhersteller in den USA unter Umständen Zulassungen nach weiteren gesetzlichen Bestimmungen einholen, darunter etwa der Health Insurance Portability and Accountability Act (kurz: HIPAA) oder der Health Information Technology for Economic and Clinical Health Act (kurz: HITECH), die die Sicherheit und den Schutz von medizinischen Daten regeln. Die Erfüllung dieser Konformitätsanforderungen ist zeitaufwendig und wirft ganz erhebliche Zusatzkosten auf dem Weg zur Marktreife auf, doch es führt kein Weg an ihr vorbei.

Aufsichtsbehörden wie die FDA prüfen zwar keine einzelnen Komponenten, sondern ganze Geräte. Dennoch ist es für den Hersteller von Vorteil, wenn seine Geräte auf einem OS aufbauen, das bereits erfolgreich in Systemen zum Einsatz kam, die den Anforderungen der Aufsichtsbehörde genügen. Und nicht nur das: Die Auswahl eines OS, dessen Konformität mit wichtigen Medizintechniknormen wie etwa IEC 62304 bereits bewiesen wurde, kann den Zeit- und Kostenaufwand für die Erlangung einer Zertifizierung erheblich reduzieren.

Konform mit IEC 62304

Die Medizingeräte-Softwarenorm IEC 62304, auf die Richtlinien der FDA (USA) sowie der Generaldirektion Gesundheit und Verbraucher (EU), insbesondere die Medizinprodukterichtlinie (93/42/EWG), die Richtlinie für aktive implantierNbare medizinische Geräte (90/385/EWG), und die Richtlinie über In-vitro-Diagnostika (98/79/EG) Bezug nehmen, be- »

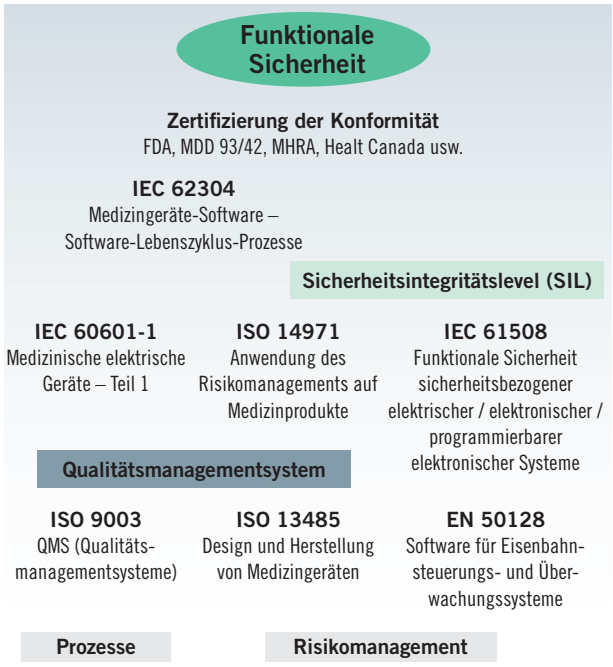

Abb. 1: Normen für funktionale Sicherheit.

	App1	App2	App3
Privilegierungsstufe	1	2	3
Systemressource:			
mmap	✔	✘	✘
exec	✘	✔	✔
fork	✔	✘	✘
ioctl	✘	✘	✔
sockets	✔	✔	✘
shmem	✘	✔	✘

Eindeutige Regelung: Granulare Zugriffsrechte und Privilegierungsstufen auf Betriebssystemebene.

schreibt empfohlene Vorgehensweisen für Hersteller, die hochwertige Software für das Gesundheitswesen entwickeln.

Die IEC 62304 ist eine der Normen, die die funktionale Sicherheit in Medizingeräten regelt (Abbildung 1). Sie geht davon aus, dass in medizintechnischen Geräten Software-Standardkomponenten („off-the-shelf", kurz: OTS, kommerziell oder anderweitig) zum Einsatz kommen, und liefert zwei Definitionen für „Software unklarer Herkunft" (SOUP): Einmal Software, die nicht speziell für ein medizinisches Gerät geschrieben wurde, und zum anderen Software mit fehlender oder unzureichender Dokumentation des Entwicklungsprozesses.

Wichtig ist an dieser Stelle, dass die Unterscheidung nicht zwischen kommerziellen Standardkomponenten (COTS) und Software unklarer Herkunft (SOUP) erfolgt, sondern zwischen undurchsichtiger (opaque) SOUP und klarer (clear) SOUP. Man kann davon ausgehen, dass Gerätehersteller, die zwischen undurchsichtiger Opaque-SOUP (die zu vermeiden ist) und Clear-SOUP (für die Sourcecode, Fehlerhistorien und Daten aus dem Langzeiteinsatz vorliegen) unterscheiden, in vielen Fällen feststellen werden, dass COTS-Software die optimale Wahl für sicherheitsrelevante Medizingeräte ist.

ISO-62304-Konformität bietet zwar zahlreiche Vorteile, in der Realität sind aber die meisten Betriebssysteme nicht konform. Es drängt sich der Vergleich eines Hauskaufs auf, bei dem nur die Fassade, nicht aber das Tragwerk des Objekts die baurechtlichen Auflagen erfüllt.

Datenleck mit schwerwiegenden Folgen

Wo im Englischen zwischen „Safety" und „Security" unterschieden wird, kennen wir im Deutschen nur ein Wort: „Sicherheit" – schließlich gehen funktionale Sicherheit (safety) und Sicherheit vor externen Bedrohungen (security) Hand in Hand. Sicherheitsbedrohungen für medizinische Geräte sind real. Systeme im Gesundheitswesen sind aufgrund ihrer Verwundbarkeit und des Werts der von ihnen verwalteten Informationen ein lohnendes Angriffsziel. Ein Datenleck bei einem medizinischen Gerät kann schwerwiegende Folgen haben: Es könnten vertrauliche Patientendaten kompromittiert werden, oder das Gerät könnte böswillig modifiziert und dadurch die Gesundheit von Patienten gefährdet werden.

Erst kürzlich hat die FDA neue Hinweise zu Cybersicherheit bei medizinischen Geräten herausgegeben. Die Hinweise enthalten Empfehlungen sowie eine Liste von Informationen, die bei Anträgen auf Marktzulassung von medizintechnischen Geräten bei der FDA beizufügen sind. Unter anderem wird den Herstellern von Medizingeräten nahegelegt, Cybersicherheits-Kontrollmechanismen zu entwickeln, die sicherstellen, dass ein Gerät seinen vorgesehenen Einsatzzweck erfüllt, und Cybersicherheit bei Konzeption und Entwicklung des Medizingeräts zu berücksichtigen. Weitere empfohlene Sicherheitsvorkehrungen sind dabei die Beschränkung des Zugriffs auf authentifizierte Benutzer, die Gewährleistung der Vertraulichkeit von Inhalten (zum Beispiel Schutz der Datenübertragungen an das und von dem Gerät) und die Implementierung von Gerätefeatures, die die kritische Funktionalität schützen.

Mehr Schutz vor Hackern

Es werden Fortschritte im Bereich des Betriebssystems angemahnt, darunter mehr Schutz vor Hackern in mobilen Netzen. Das Betriebssystem muss eine wesentlich feingranularere Kontrolle über mehrere Systemprivilegierungsstufen bieten. Systementwickler sollten über Einstellungen festlegen können, welche Operationen ein Programm ausführen und wie es einen Dienst vom Kernel des Betriebssystems anfordern darf. Außerdem sollte es nicht mehr erforderlich sein, einem Softwareprogramm, das nur bestimmte Ressourcen benötigt, Root-Zugriff auf das ganze System zu geben. Vielmehr sollte das Betriebssystem den Systementwickler festlegen lassen, welche Ressourcen ein Programm exakt benötigt, und den Zugriff auf andere Ressourcen sperren.

Da sich Ärzte und Patienten immer mehr auf mobile medizinische Geräte und medizinische Apps verlassen, werden Maßnahmen für mehr Datenschutz und Sicherheit immer wichtiger. Die Wahl des Betriebssystems hat erhebliche Auswirkungen auf die möglichen Sicherheitsmaßnahmen wie auch auf den Zeit- und Kostenaufwand für die Zertifizierung und die Gesamtkosten des Geräts.

Chris Ault
ist Senior Product Manager für das Medizintechnik-Softwareportfolio von QNX Software Systems.

Alle Bilder: QNX