Sicher zukunftssicher: Medizingeräteentwicklung mit (Cyber-)Security im Fokus



Die richtige Technologieentscheidung wird immer wichtiger: Medizintechnikunternehmen stehen bei der Entwicklung eines Nachfolgegerätes oder einer Neuentwicklung häufig vor der Frage, welche Technologie die geeignete Grundlage für das zukünftige Produkt bildet. Soll auf neue Technologien und aktuelle Trends gesetzt werden oder ist eine bewährte technische Plattform die bessere Wahl?

Eine solche Entscheidung muss zahlreiche Aspekte berücksichtigen. Neben Rechenleistung, Energieverbrauch, Schnittstellen und Kosten spielen insbesondere die langfristige Verfügbarkeit, die Softwareunterstützung, die funktionale Sicherheit und aktuell besonders die Cybersecurity eine entscheidende Rolle.

Gerade bei medizinischen Geräten sind Fehlentscheidungen besonders kritisch. Die Entwicklung ist mit umfangreichen regulatorischen Anforderungen, aufwendigen Verifikations- und Validierungsprozessen sowie häufig kostspieligen Zulassungsverfahren verbunden. Wird die technische Plattform während der Entwicklung geändert, können sich dadurch erhebliche zusätzliche Aufwände ergeben.

Autor:
Konrad Zöpf
Produkt Manager
TQ-Group
www.tq-group.com

Anforderungen durch neue Technologien

Gleichzeitig halten neue Technologien wie künstliche Intelligenz (KI), maschinelles Lernen (ML), leistungsfähige Grafikprozessoren (GPUs) und Neural Processing Units (NPUs) zunehmend Einzug in medizinische Anwendungen. Auch die Vernetzung von Geräten über Wi-Fi, Bluetooth, Mobilfunk oder Ethernet nimmt weiter zu.

Damit entstehen neue Möglichkeiten, aber auch neue Anforderungen: Je stärker ein Medizingerät vernetzt und softwarebasiert ist, desto wichtiger wird die Frage, wie Verfügbarkeit, Integrität und Vertraulichkeit der Systeme und Daten über den gesamten Produktlebenszyklus gewährleistet werden können.

Vernetzung bringt neue Chancen und Risiken

Drahtlose Schnittstellen können die Bedienung und den Einsatz medizinischer Geräte erheblich vereinfachen. Aufwendige Verkabelungen lassen sich reduzieren, Diagnoseeinheiten können flexibler eingesetzt werden und Patienten profitieren von einer höheren Mobilität bei der Erfassung und Übertragung medizinischer Daten.

Gleichzeitig erweitert jede zusätzliche Kommunikationsschnittstelle die Angriffsfläche eines Systems. Ein Gerät, das über Wi-Fi, Bluetooth oder ein Netzwerk mit anderen Systemen kommuniziert, muss nicht nur funktional zuverlässig arbeiten. Es muss auch gegen unbefugten Zugriff, Manipulation und die Ausnutzung von Schwachstellen geschützt werden.

Cybersecurity ist deshalb nicht als nachträgliche Ergänzung zu verstehen. Sie sollte bereits bei der Definition der Systemarchitektur berücksichtigt werden. Dazu gehören beispielsweise eine geeignete Zugriffskontrolle, sichere Kommunikationsverbindungen, ein abgesicherter Boot-Prozess, der Schutz von Schlüsseln und Zugangsdaten sowie die Möglichkeit, Software und Firmware sicher zu aktualisieren.

Für die Medizintechnik kommt hinzu, dass ein Security-Vorfall im ungünstigsten Fall nicht nur einen Datenverlust oder einen Produktionsausfall verursachen kann. Je nach Funktion des Gerätes können Verfügbarkeit und Integrität unmittelbaren Einfluss auf die Patientensicherheit haben.

Interoperabilität als wichtiger Bestandteil moderner Medizintechnik

Neben der Vernetzung gewinnt auch die Interoperabilität medizinischer Geräte und Systeme zunehmend an Bedeutung. Der Datenaustausch zwischen verschiedenen Geräten ermöglicht einen schnellen Zugriff auf wichtige Informationen und kann dadurch Diagnostik und Behandlung unterstützen.

Bei Software umfasst die syntaktische Interoperabilität unter anderem die Verwendung gleicher Datenformate und Kommunikationsprotokolle. Je besser verschiedene Systeme miteinander kommunizieren können, desto geringer ist der Aufwand für die Integration.

Mit der zunehmenden Vernetzung muss allerdings auch die Security der Schnittstellen betrachtet werden. Offene und standardisierte Schnittstellen bieten Vorteile für die Interoperabilität, dürfen aber nicht dazu führen, dass unzureichend geschützte Kommunikationswege entstehen.

Die Architektur eines modernen Medizingerätes muss daher mehrere Ziele gleichzeitig erfüllen: Sie muss leistungsfähig, interoperabel, sicher, wartbar und langfristig verfügbar sein.

Die Auswahl des Betriebssystems ist eine strategische Entscheidung

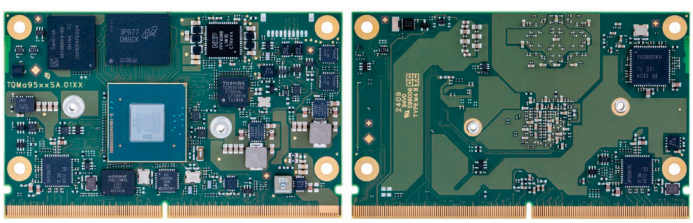
Die Auswahl der geeigneten Software – und insbesondere des Betriebssystems – ist deshalb ein wesentlicher Bestandteil der Geräteentwicklung. Bei ARM-basierten Prozessoren steht eine große Auswahl unterschiedlicher Betriebssysteme zur Verfügung. Neben Linux und Android können je nach Anwendung auch Betriebssysteme wie QNX oder PikeOS eingesetzt werden.

Insbesondere bei Anwendungen mit hohen Anforderungen an funktionale Sicherheit und Security können entsprechende Betriebssystemkonzepte Vorteile bieten.

Security

Für die Security ist dabei nicht nur die reine Betriebssystemfunktionalität relevant. Entscheidend ist auch, wie lange das Betriebssystem gepflegt wird, wie schnell Sicherheitsupdates zur Verfügung stehen und welche Möglichkeiten für einen sicheren Update-Prozess bestehen.

Ebenso wichtig ist die Unterstützung der im Prozessor integrierten Security-Funktionen. Moderne ARM-basierte Prozessoren verfügen je nach Plattform beispielsweise über Funktionen zur Absicherung des Boot-Prozesses, zur sicheren Speicherung von Schlüsseln oder zur Trennung unterschiedlicher Ausführungsumgebungen.



Hypervisor-Lösungen

Ein weiterer interessanter Ansatz sind Hypervisor-Lösungen. Hier können mehrere Betriebssysteme oder Ausführungsumgebungen auf einem Multicore-System voneinander getrennt betrieben werden. Dadurch lässt sich beispielsweise ein sicherheitskritischer Teil des Systems von weniger vertrauenswürdigen oder stärker vernetzten Komponenten logisch isolieren.

Eine solche Trennung kann insbesondere dann interessant sein, wenn unterschiedliche Anforderungen an Safety und Security innerhalb eines Systems erfüllt werden müssen. Sie ersetzt jedoch kein systematisches Risikomanagement: Auch zwischen den getrennten Bereichen müssen Schnittstellen eindeutig definiert und abgesichert werden.

Damit gewinnt das Software-Lifecycle-Management an Bedeutung. Für ein medizinisches Gerät reicht es nicht aus, dass die Software zum Zeitpunkt der Markteinführung sicher erscheint. Auch während der erwarteten Nutzungsdauer müssen Schwachstellen erkannt, bewertet und – soweit erforderlich – durch geeignete Maßnahmen behandelt werden.

Security beginnt bei CPU und Embedded-Modul

Die Entscheidung für eine bestimmte CPU oder ein Embedded-Modul sollte deshalb nicht ausschließlich anhand von Rechenleistung, Preis und Schnittstellen getroffen werden.

Bereits bei der Auswahl der Hardwareplattform sollte geprüft werden, welche Security-Funktionen die CPU bereitstellt und wie diese durch das Board Support Package (BSP), das Betriebssystem und die Firmware unterstützt werden.

Von Bedeutung sind unter anderem:

- Secure Boot und eine Vertrauenskette vom Start des Systems bis zur Applikation,
- Hardware-basierte Funktionen zum Schutz kryptografischer Schlüssel,
- sichere Firmware- und Software-Updates,
- Möglichkeiten zur Authentifizierung und Zugriffskontrolle,
- Trennung unterschiedlicher Softwarekomponenten,
- Absicherung von Debug- und Service-Schnittstellen,
- langfristige Versorgung mit Sicherheitsupdates,
- nachvollziehbares Versions- und Konfigurationsmanagement.

Für den Entwickler ist dabei insbesondere die Frage wichtig, welche dieser Funktionen tatsächlich in der eigenen Systemarchitektur genutzt werden können.

Ein Hersteller kann sich nicht allein darauf verlassen, dass eine CPU grundsätzlich über Security-Funktionen verfügt. Entscheidend ist vielmehr, ob diese Funktionen dokumentiert, verfügbar, softwareseitig unterstützt und für die konkrete Anwendung nutzbar sind.

Cybersecurity und regulatorische Anforderungen

Die zunehmende Bedeutung von Cybersecurity spiegelt sich auch in der europäischen Regulierung wider. Für Medizinprodukte sind insbesondere die Anforderungen aus der Medizinprodukteverordnung (MDR) und für In-vitro-Diagnostika aus der IVDR relevant. Die europäische Leitlinie MDCG 2019-16 behandelt ausdrücklich die Cybersecurity von Medizinprodukten und stellt Cybersecurity in den Zusammenhang mit Entwicklung, Risikomanagement und dem gesamten Produktlebenszyklus.

Parallel dazu ist mit dem Cyber Resilience Act (CRA), der Verordnung (EU) 2024/2847, ein horizontaler europäischer Rechtsrahmen für Produkte mit digitalen Elementen geschaffen worden. Der CRA formuliert unter anderem Anforderungen an die Cybersicherheit bei Design, Entwicklung und Produktion sowie an Prozesse zur Behandlung von Schwachstellen während der erwarteten Nutzungsdauer eines Produktes.

Wann ist der CRA zu beachten?

Für die Medizintechnik ist dabei eine wichtige Abgrenzung erforderlich: Der CRA gilt ausdrücklich nicht für Produkte mit digitalen Elementen, auf die unter anderem die MDR oder die IVDR Anwendung findet. Medizinprodukte werden daher nicht einfach zusätzlich dem CRA unterworfen.



Dennoch ist der CRA für die technische Plattform- und Lieferkettenbetrachtung relevant. Hersteller und Entwickler sollten bereits bei der Auswahl von Software, Embedded-Modulen und digitalen Komponenten prüfen, welche regulatorischen Anforderungen für das jeweilige Produkt und seine Komponenten gelten und welche Security-Prozesse durch die Lieferanten unterstützt werden.

Die regulatorische Betrachtung darf daher nicht erst kurz vor der Markteinführung beginnen. Sie sollte bereits bei der Auswahl der technischen Plattform Bestandteil der Entwicklungsstrategie sein.

Secure by Design statt nachträgliche Ergänzung

Eine wesentliche Konsequenz aus dieser Entwicklung ist der Übergang von einer nachträglichen Absicherung zu einem konsequenten „Security by Design"-Ansatz. Security-Anforderungen sollten bereits während der Systemdefinition festgelegt werden. Dazu gehört zunächst eine Betrachtung möglicher Bedrohungen und Angriffspunkte. Anschließend müssen geeignete technische und organisatorische Maßnahmen definiert und während der Entwicklung verifiziert werden.

Für Embedded-Systeme betrifft dies beispielsweise den Boot-Prozess, die Firmware, das Betriebssystem, Kommunikationsschnittstellen und die Applikation.

Update-Fähigkeit

Auch die Update-Fähigkeit sollte frühzeitig berücksichtigt werden. Ein Gerät mit einer erwarteten vieljährigen Nutzungsdauer benötigt eine Strategie für den Umgang mit neuen Schwachstellen. Ein Sicherheitsupdate muss dabei nicht nur technisch verfügbar sein, sondern auch sicher verteilt, installiert und verifiziert werden können.

Eine weitere Herausforderung ist die Verwendung von Software von Drittanbietern und Open-Source-Komponenten. Je komplexer die Software eines Produktes wird, desto wichtiger wird eine nachvollziehbare Übersicht über die verwendeten Komponenten und deren Versionen. Eine Software Bill of Materials (SBOM) kann dabei eine wichtige Grundlage für Transparenz und Schwachstellenmanagement darstellen.

Embedded-Module und SBCs als Entwicklungsgrundlage

Embedded-Module und Single Board Computer (SBCs) können hier eine geeignete Grundlage für die Entwicklung medizinischer Geräte darstellen. Sie stellen bereits zahlreiche Hardware- und Softwarefunktionen bereit und können dadurch Entwicklungszeit und Entwicklungsrisiken reduzieren.

Der Entwickler kann sich stärker auf die applikationsspezifischen Anforderungen konzentrieren, während grundlegende Funktionen der Plattform bereits vorhanden sind.

Arm-basierte Lösungen bieten dabei eine große Bandbreite an Rechenleistungen und unterstützen zahlreiche Schnittstellen. Moderne Multicore-Systeme können zudem unterschiedliche Prozessorfunktionen und Beschleuniger integrieren - dazu zählen neben Grafik- und Multimediafunktionen auch NPUs für KI-Anwendungen und hardwarebasierte Security-Funktionen.

Für die Entwicklung medizinischer Geräte ist jedoch entscheidend, dass die technischen Möglichkeiten auch in eine belastbare Systemarchitektur überführt werden können. Ein Embedded-Modul sollte deshalb nicht allein danach ausgewählt werden, was die Hardware heute leisten kann. Ebenso relevant ist, welche Möglichkeiten die Plattform für sichere Softwarearchitekturen, Updates, Wartung und langfristige Weiterentwicklung bietet.

Fazit: Die Plattformentscheidung ist strategisch

Embedded-Systeme bieten für die Entwicklung moderner Medizingeräte zahlreiche Vorteile. Sie verbinden Energieeffizienz, Rechenleistung, eine große Auswahl an Softwarelösungen und Entwicklungstools mit einer hohen Flexibilität. Gleichzeitig steigen die Anforderungen an moderne medizinische Geräte. KI, ML, drahtlose Kommunikation und Interoperabilität eröffnen neue Möglichkeiten, erhöhen aber auch die technische und regulatorische Komplexität. Cybersecurity muss deshalb zu einem integralen Bestandteil der Plattformauswahl und Systementwicklung werden.

Für Entwickler bedeutet dies: Nicht nur die Leistungsfähigkeit eines Prozessors oder die Anzahl der Schnittstellen entscheidet über die Eignung einer Plattform. Ebenso wichtig sind sichere Hardwarefunktionen, die Softwareunterstützung, Updatefähigkeit, Schwachstellenmanagement und die langfristige Verfügbarkeit der gesamten Plattform.

Auch regulatorische Entwicklungen wie der Cyber Resilience Act unterstreichen die zunehmende Bedeutung eines systematischen Umgangs mit Cybersecurity. Für Medizinprodukte selbst ist dabei die Abgrenzung zu den sektorspezifischen Anforderungen der MDR und IVDR entscheidend.

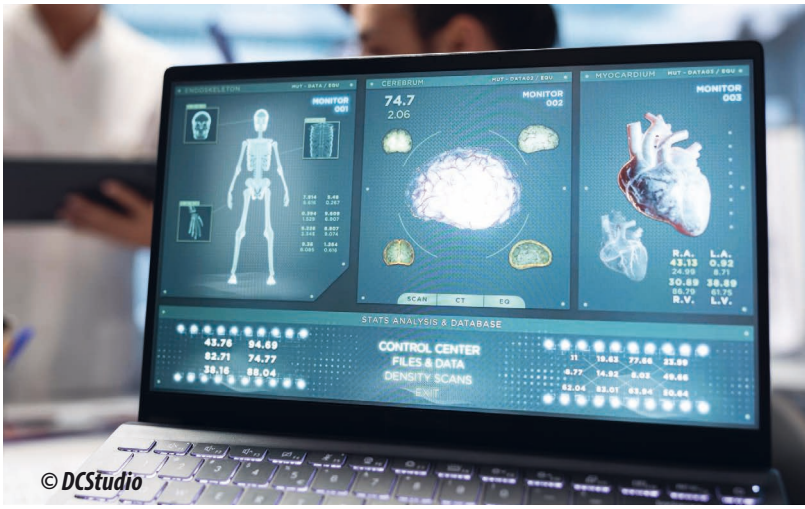
Der CRA gilt grundsätzlich ab dem 11. Dezember 2027; bestimmte Pflichten greifen bereits früher, darunter die Meldepflichten für aktiv ausgenutzte Schwachstellen und schwerwiegende Sicherheitsvorfälle seit dem 11. September 2026.

Für Medizintechnikhersteller ist deshalb eine frühzeitige Auseinandersetzung mit Security sinnvoll – nicht erst im Rahmen der Zulassung oder kurz vor dem Produktstart.

Zukunftssichere medizinische Geräte

Wer bei der Auswahl von CPU, Embedded-Modul, Betriebssystem und Softwareplattform bereits heute auf langfristige Wartbarkeit und Security achtet, schafft damit eine wesentlich bessere Grundlage für zuverlässige, effiziente und zukunftssichere medizinische Geräte.

Gerade der Einsatz bewährter und langfristig verfügbarer Embedded-Module und SBCs kann dabei helfen, Entwicklungszeiten zu reduzieren und Risiken zu minimieren. Entscheidend ist jedoch, dass die Plattform nicht nur technisch leistungsfähig, sondern auch über die gesamte geplante Produktlebensdauer beherrschbar und sicher betreibbar ist.



© DCStudio

Wer schreibt:

Konrad Zöpf ist staatlich geprüfter Techniker und arbeitete nach seiner Ausbildung als Medizintechniker und Applikationsingenieur bei zwei Medizintechnik-Unternehmen. Seit mittlerweile 26 Jahren ist er bei der TQ-Group tätig, zunächst in der Elektronik-Entwicklung sowie seit gut sechszehn Jahren als Produktmanager in der Embedded-Sparte.

Er verantwortet bei TQ die ARM- und Layerscape-Produktpalette. Seit Anfang 2020 ist er zusätzlich stellvertretender Bereichsleiter für TQ-Embedded. ◄