Elektronik medical

Innovative Produkte und Lösungen für die Medizintechnik

E-Health & Security

Immun gegen Angriffe

Seite 39

Bild: mimi/stock.adobe.com

Top 5

Elektronischer Beipackzettel

In unserem elektronischen Beipackzettel präsentieren wir Ihnen die Top 5 der meistgelesenen Onlineartikel der Elektronik medical der vergangenen Wochen.

UMBAU ZUM DIGITALKONZERN

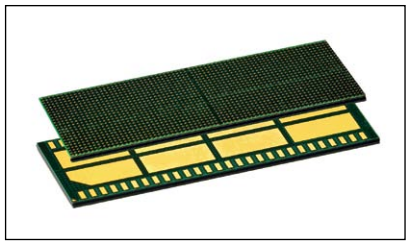
(Bild: Siemens Healthineers)

Siemens ohne Healthineers? Chancen für Medizintechnik-Abspaltung

Kommt eine Abspaltung vom Mutterkonzern noch 2025? Siemens erwägt, die Anteile an seiner Medizintechniksparte zu verkaufen, zugunsten der digitalen Industrie. Eine Entscheidung wird für Dezember erwartet. Was sind die Hintergründe und was bedeutet der Schritt für Healthineers?

SYSTEM-IN-PACKAGE VON AMS OSRAM

(Bild: ams Osram)



Photon Counting: Neues CT-Sensormodul für Bildgebung der Zukunft

ams Osram hat ein neuartiges Plug-and-Play-Sensormodul für die Computertomographie vorgestellt. Die hochintegrierte und robuste Detektortechnik lässt sich über ein »4-side buttable System-in-Package« leicht handhaben, für höchste Bildqualität in photonenzählenden CT-Scannern.

VOM STARTUP ZUM BÖRSENASPIRANTEN

(Bild: Brainlab)

IPO im Herbst: Geht Brainlab an die Börse?

Marktkapitalisierung nach Rückzug des Gründers Stefan Vilsmeier: Brainlab scheint für die zweite Jahreshälfte einen Börsengang in Frankfurt anzustreben. Das Münchner Unternehmen für Medizintechniksoftware und OP-Planung könnte mit rund zwei Milliarden Euro bewertet werden.

DIAGNOSE PER LICHT UND SCHALL

(Bild: Trumpf / iThera)

Neue Trumpf-Lasertechnik untersucht Weichgewebe und Blutfluss

Trumpf Photonic und iThera Medical haben eine neue laserbasierte Diagnosetechnik für die optoaktustische Bildgebung vorgestellt. Das VCSEL-Lasersystem ist 100-mal kleiner und stromsparender, läuft in Laserklasse 1 und soll dank detaillierter Bilder herkömmliche Diagnosesysteme ersetzen.

NEUE STRATEGISCHE AUSRICHTUNG

(Bild: Biotronik)

Biotronik setzt auf aktive Implantate und digitale Gesundheit

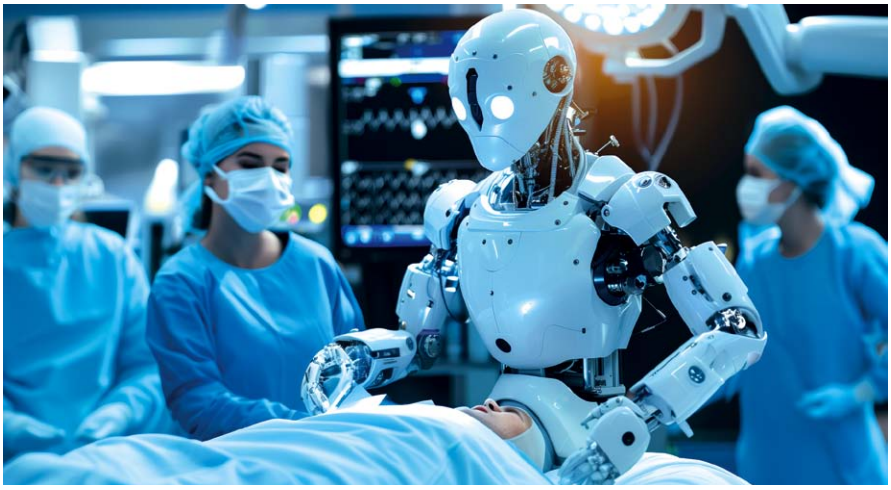
Der Medizintechnikhersteller Biotronik stellt sich strategisch neu auf. Um seine Position bei aktiven Implantaten wie Herzschrittmachern und digitalen Gesundheitsprodukten zu stärken, wird unter anderem der Geschäftsbereich »Vaskuläre Intervention« (VI) an Teleflex verkauft.

Ambient Computing für Krankenhäuser

Microsoft Dragon Copilot: KI-Assistent soll Kliniken entlasten

Von der Spracherkennung zum kontextsensiblen Assistenten – der von Microsoft pünktlich zur HIMSS 2025 in Las Vegas vorgestellte Dragon Copilot ist die logische Weiterentwicklung der in Kliniken etablierten Dragon-Medical-One-Spracherkennungs-Software (DMO) und der aktuellen Copilot-Initiativen. Wie einst Microsoft Office in die Büros soll nun die KI in Kliniken und Praxen einziehen. Die Software wird voraussichtlich ab Sommer in Europa verfügbar sein. Ziele sind nicht nur eine effizientere Organisation und Verwaltung, sondern auch die Verbesserung der Arzt-Patienten-Beziehung durch mehr Zeit und den Fokus auf den menschlichen Kontakt.

Das KI-System kombiniert die medizinische Spracherkennung mit der Copilot-Plattform DAX für automatisierte Aufgaben, Dokumentation und smarte Recherche – und soll so Personalmangel und Dokumentationslast senken. Während die ursprünglich von Nuance entwickelte DMO auf präzise Sprache-zu-Text-Transkription spezialisiert war, erweitert die Integration der DAX-Copilot-Plattform die Fähigkeiten um Ambient Computing: Die KI analysiert also natürliche Gespräche zwischen Medizinern und Patienten in Echtzeit, extrahiert relevante klinische Daten und generiert automatisch strukturierte Berichte.



Was Microsofts Klinik-Copilot kann

Das »mithörende« Produkt von Microsoft bietet eine einheitliche Benutzeroberfläche für Funktionen wie »Umgebungsdokumentation«, »Entscheidungsunterstützung« und »Workflow-Automatisierung«.

- **Umgebungsdokumentation:** Bei Patientengesprächen transkribiert die KI nicht nur Sprache, sondern erkennt diagnostische Schlüsselinformationen, Medikationspläne und Behandlungsziele. Fallbezogene Notizen, Überweisungsschreiben und Epikrisen werden automatisch generiert – unterstützt durch mehrsprachige Funktionen und anpassbare Vorlagen.
- **Klinische Entscheidungsunterstützung:** Ein eingebetteter Recherche-Assistent durchsucht evidenzbasierte Quellen wie »UpToDate« und »PubMed« und stellt kontextrelevante Studien oder Leitlinien bereit, ohne dass die Behandelnden die Oberfläche der digitalen Patientenakte verlassen müssen.
- **Workflow-Automatisierung:** Routine-Tasks wie Laboranforderungen, Rezeptausstellungen oder Terminverfolgung werden per Sprachbefehl initiiert. Ein Highlight ist laut Microsoft die »Conversational-Orders«-Funktion, bei der die KI aus freier Sprache präzise Arbeitsaufträge für Pflegepersonal oder Fachabteilungen ableitet.

Was die Dragon-KI Ärzten und Patienten verspricht

Burnout-Prävention durch weniger Bürokratie: Laut aktuellen Microsoft-Daten berichten 70 Prozent der DAX-Copilot-Nutzer über geringere Erschöpfung, diesen Effekt könnte die Dragon-KI verstärken: Pilotstudien zeigen fünf Minuten Zeitersparnis pro Patientenkontakt – bei 20 Konsultationen täglich wären dies über 16 Arbeitsstunden im Monat. Auch die Behandlungsqualität soll profitieren: 93 Prozent der Patienten in DAX-Pilotprojekten bewerten die Interaktion mit KI-unterstützten Ärzten positiver. Grund dafür ist deren ungeteilte Aufmerksamkeit während der Visite.

In den USA kooperiert Microsoft für eine nahtlose Integration mit EHR-Anbietern (Electronic Health Record) wie Epic und Cerner, für bestehende DMO-Kunden ist ein migrierter Support vorgesehen. Für hohe Datensicherheit und den verantwortungsvollen KI-Umgang verweist der US-Software-Gigant auf seine »Responsible AI«-Prinzipien Transparenz, Fairness und Compliance. Zum einen erhalten Kliniker damit Einblick in die Datenquellen der KI-Empfehlungen. Zum zweiten wurden die Algorithmen mit diversen Sprachdatensätzen trainiert, um Dialekte und Akzente zu verstehen. Eine isolierte Datenverarbeitung innerhalb der Microsoft Cloud for Healthcare stellt die HIPAA- und GDPR-Konformität sicher. Zudem blockiert das System nicht verifizierbare Diagnosevorschläge.

Skalierung und Wearable-Schnittstellen

Obwohl zunächst auf stationäre und ambulante Versorgung zugeschnitten, sieht Microsoft weitere Szenarien in Pflegeheimen, Reha-Einrichtungen und der Telemedizin. Interessant ist die geplante Schnittstelle zu Wearables: Vitaldaten von Smartwatches könnten zukünftig automatisch in die KI-Dokumentation einfließen.

Für die Unterstützung von Ärzten bei der Umstellung von manueller Dokumentation auf KI-gestützte Prozesse setzt Microsoft auf Trainingsprogramme zertifizierter Partner. Bezüglich möglicher Fehlinformationen seitens der KI-Tools betont der Software-Konzern, dass der Dragon Copilot lediglich assistiert und keine autonomen Entscheidungen trifft – also immer eine Ärztin oder eine medizinische Fachkraft das letzte Wort behält. (uh)

Neuer Architektur-Ansatz für medizinisches Halbleiter-Design

On-Chip-Sicherheit für die Medizin

Vertrauenswürdige Plattform-Chips für vernetzte Medizingeräte: Das Barkhausen Institut hat ein »Netzwerk on Chip« entwickelt, welches einzelne Halbleiterkomponenten über Wächtereinheiten verbindet – und so höchste Sicherheit, eine flexible Entwicklung sowie individuelle Medizin-Chips in Massenfertigung ermöglicht.

Von Michael Roitzsch
Barkhausen Institut

Bild: Arifin Studio/stock.adobe.com

Die Digitalisierung gilt als einer der größten Treiber für die Medizintechnik und die Gesundheitsversorgung der Zukunft: Verbesserungen bei Diagnose und Behandlung sind zunehmend an Software und entsprechende digitale Hardware geknüpft. Medizingeräte für den Einsatz direkt am oder nahe dem Patienten stellen Medtech-Hersteller, deren Elektronikzulieferer und die Ingenieure und Entwickler vor vielfältige Herausforderungen. Digitale Halbleiterchips für diagnostische und therapeutische Geräte in den Behandlungsräumen müssen den zahlreichen Anforderungen des medizinischen Alltags, allen geltenden Normen und Zertifizierungen wie auch hohen Sicherheitsaspekten genügen.

Spannungsfelder für digitale Hardware

Als »Always-On«-Devices mit Cloud-Anbindung müssen (künftige) Medizingeräte auf der einen Seite sehr sicher, aber auch energieeffizient und thermisch stabil sein – was gerade bei den für KI benötigten rechenstarken Prozessoren eine Herausforderung darstellt. Für digitale Chips in Medizingeräten gelten daher drei entscheidende Spannungsfelder:

- Rechenleistung und Stromverbrauch
- Maßanfertigung und Kosteneffizienz
- Flexibilität und Sicherheit

Power versus Processing

Die von der Hardware bereitgestellte Rechenleistung und auch die Kommunikationsfähigkeiten über drahtgebundene oder drahtlose Schnittstellen entscheiden darüber, welche Anwendungsfälle mit einem Chip umsetzbar sind. Dafür enthalten die Chips Prozessoren und andere Recheneinheiten zum Ausführen von Programmen, aber auch Techniken wie Mobilfunk oder WLAN für die Kommunikation mit der Außenwelt. Ein Mehr an Rechenleistung auf Chip-Ebene ermöglicht fortschrittlichere Programme, allerdings zum Preis eines er-

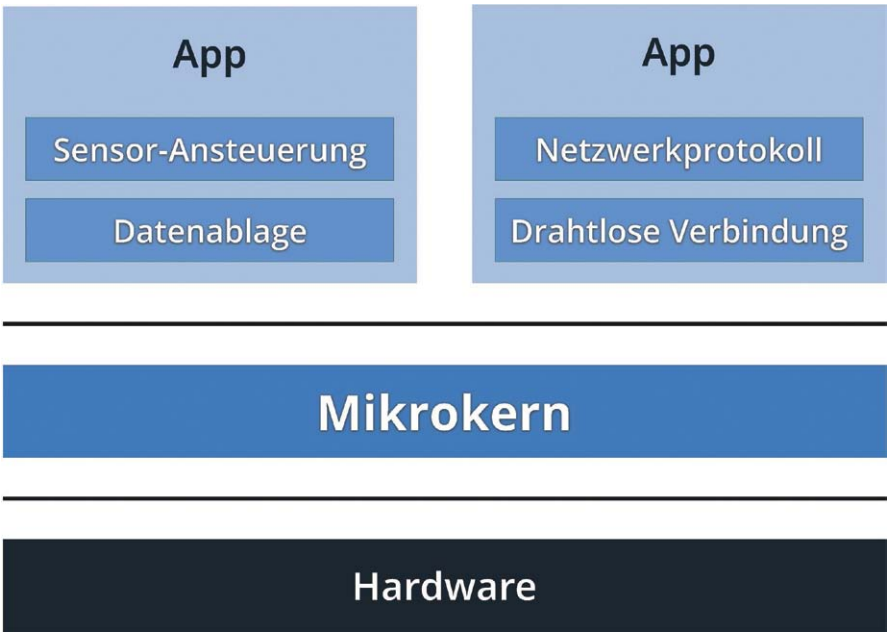


Bild 1. In der M³-Architektur liegen die Anwendungsfunktionen in isolierten Bereichen, Fehler in einer Anwendung schaden den anderen nicht. Der Mikrokern dient als abgesicherte Isolationsschicht. (Bild: Barkhausen Institut)

höhten Stromverbrauchs. Batteriebetrieb und Hitzeentwicklung von tragbaren oder gar im Körper einsetzbaren Produkten setzen dem Stromverbrauch enge Grenzen.

Customized Chip-Sets aus Serienproduktion

Die Vielfalt von aktuellen oder in Zukunft denkbaren Medizingeräten erfordert jeweils auf den Anwendungsfall zugeschnittene Chip-Fähigkeiten. Einer separaten Maßanfertigung für jedes Gerät steht jedoch die Kosteneffizienz entgegen. Chip-Fertigung wird erst bei sehr großen Stückzahlen kosteneffektiv, daher sind dedizierte Chips für Medizingeräte mit geringen Seriengrößen wirtschaftlich nicht tragbar. Insbesondere zur einmaligen Verwendung am Patienten konzipierte Wegwerf-Geräte müssen jedoch günstig herzustellen sein, um das Gesundheitssystem nicht unnötig zu belasten.

On-Chip-Security

Ein drittes Spannungsfeld eröffnet sich zwischen der Flexibilität durch Aktualisierung von Software und der Zertifizierbarkeit und Sicherheit der Geräte. Software ist schnelllebig, und in digitalen Produkten können neue Erkenntnisse und Funktionen prinzipiell durch Aufspielen einer neuen Version der Software umgesetzt werden. Auch im Medizinbereich wäre es aus Kosten- und Nachhaltigkeitsgründen wünschenswert, wenn ein kostspielig entwickeltes und beschafftes Gerät durch neue Software-Versionen aktuell gehalten und damit länger genutzt werden kann. Allerdings unterliegen Medizingeräte Regulierungen, welche oftmals eine Zertifizierung voraussetzen. Eine Aktualisierung der Software würde dann eine erneute Zertifizierung erfordern, was wiederum die Kosten in die Höhe treibt. Diese regulatorischen Prozesse sind jedoch eine Grundlage des Vertrauens, welches Patienten in die verwendete Technik setzen.

Chip-Architektur für alle Medizinszenarien

Angewandt auf die drei Spannungsfelder eröffnen sich Ansätze für Lösungen: Das Bereitstellen von hoher Rechenleistung erfordert die Integration von leistungsstarken Prozessoren auf dem Chip. Um den Stromverbrauch zu senken, werden diese Prozessoren von Beschleuniger-Einheiten bei bestimmten Teilaufgaben unterstützt. Solche Beschleuniger sind auf konkrete Teilschritte wie Bildverarbeitung, Signalaufbereitung oder künstliche Intelligenz spezialisiert und bearbeiten diese Schritte mit einer höheren Energieeffizienz als Standardprozessoren. Ein offenes Problem ist dabei die Verknüpfung von Standardprozessoren und Beschleunigern, so dass diese ohne Datentransfer- und Kommunikationsverluste möglichst reibungslos zusammenarbeiten können.

Baukasten-Prinzip für Wunsch-Konfiguration

Medizingeräte für unterschiedliche Anwendungsfälle werden jedoch unterschiedliche Beschleuniger benötigen. Eine individuelle Chip-Fertigung für jedes Gerät, angepasst an dessen spezifisches Anwendungsgebiet, würde zu einer stark fragmentierten Chip-Landschaft führen. Dies hätte zur Folge, dass jede Serie nur in kleinen Stückzahlen produziert werden könnte – ein ineffizienter und kostspieliger Ansatz. Stattdessen bietet sich die Entwicklung universeller Chip-Designs an, die als Baukasten fungieren und verschiedene Beschleuniger sowie Prozessoren integrieren. Für eine spezifische Anwendung wird dann lediglich eine Teilmenge dieser Bausteine aktiviert. Dieser modulare Ansatz ermöglicht nicht nur eine effizientere Großserienfertigung und damit Kostensenkungen, sondern gewährleistet auch Flexibilität für unterschiedliche Einsatzbereiche. Dabei ist es essenziell, dass ungenutzte Chip-Komponenten weder die Funktionalität beeinträchtigen noch Sicherheitsrisiken darstellen.

Bleibt zuletzt das Problem der Flexibilität durch Software-Updates. Im Sinne der Zukunftsfähigkeit und Langlebigkeit von Geräten sind solche Updates wünschenswert. Im Sinne der Zertifizierung muss jedoch sichergestellt werden, dass Kerneigenschaften des Medizingeräts unverändert über alle Updates hinweg erhalten bleiben. So kann zum Beispiel in einem Endoskop die Bildverarbeitung durch ein Update verbessert werden, aber die Betriebssicherheit des Geräts und die Vertraulichkeit der Patientendaten müssen stets gewahrt bleiben. Dafür muss eine Chip- und Betriebssystem-Architektur geschaffen werden, die es erlaubt unveränderliche und veränderliche Bestandteile so zu kombinieren, dass die Unveränderbarkeit der Kerneigenschaften gesichert ist und im Rahmen einer Zertifizierung überprüft werden kann.

Medizinsichere Chip-Architektur M³

Das Dresdner Barkhausen Institut hat unter dem Projektnamen M³ vertrauenswürdige Plattform-Chips und einen neuen Archi-

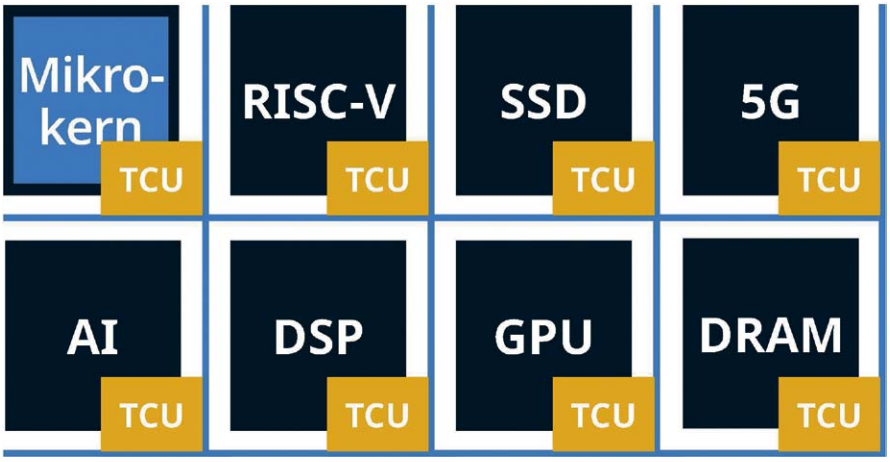


Bild 2. Basis des medizinsicheren Chip-Designs sind Trusted Communication Units (TCU), die als überprüfbare Wächterkomponenten dafür sorgen, dass Fehler in einem Hardware-Baustein andere Komponenten nicht beeinflussen. (Bild: Barkhausen Institut)

tekturansatz für das medizinische Chip-Design entwickelt, der als Brücke zwischen Sicherheit, Kommunikation und Halbleitertechnik die Anforderungen vernetzter Digital-Health-Systeme widerspiegelt. Die Grundprinzipien entstammen der Welt der Betriebssysteme, speziell der Mikrokernsysteme.

Betriebssysteme dienen allgemein als Verwaltungseinheit, welche die von der Chip-Hardware bereitgestellte Rechenkapazität an darauf laufende Programme zuteilt. Bekannte Betriebssysteme wie Windows und Linux bieten darüber hinaus eine große Palette an weiteren Funktionen, über Datenhaltung und Netzkommunikation bis zur Ansteuerung einer grafischen Oberfläche. Diese umfangreichen Funktionen erweitern die Angriffsfläche des Systems um ein Vielfaches.

Die Idee eines Mikrokernsystems ist es, die Aufgaben des Betriebssystems auf seine Kernaufgabe des Bereitstellens von Rechenkapazität zu reduzieren. Dadurch verringert sich die Angriffsfläche um ein Vielfaches. Zusatzfunktionen wie Kommunikation, Datenhaltung und grafische Ausgabe müssen dann zwar auf Anwendungsebene realisiert werden, die Isolation verschiedener Programme auf einem Mikrokernsystem wird durch die geringere Angriffsfläche aber verbessert. Die Robustheit gegenüber Programmierfehlern und die Sicherheit gegenüber digitalen Angriffen steigen. Es entsteht ein System mit dem Mikrokern als einer widerstandsfähigen und überprüfbaren Isolationsschicht und den Programmen, die so voreinander geschützt sind, dass Fehler in einem Programm ein anderes nicht beeinflussen können.

Mikrokernsystem für Halbleiter-Chips

Das Konzept des Mikrokerns ist seit den 1970er-Jahren bekannt und wird heute in Anwendungsbereichen mit höchsten Sicherheitsanforderungen industriell genutzt. Der Forschungsansatz der M³-Plattform des Barkhausen Instituts ist es, dieses Konzept auf eine Chip-Architektur zu übertragen. In herkömmlichen Hardware-Architekturen werden die verschiedenen, auf einem Chip integrierten Prozessoren und Beschleuniger durch Zugriff auf gemeinsamen Speicher miteinander verbunden. Dabei muss der gesamten Hardware vollständig vertraut werden. Sobald sich in die Implementierung eines Prozessors oder Beschleunigers ein Fehler einschleicht, kann darüber Vollzugriff auf das gesamte System erlangt werden. In den letzten Jahren sind solche Hardware-Fehler wiederholt aufgetreten. Das ist im Sinne der Sicherheit gegenüber Angriffen aber auch bezüglich der Robustheit des Systems keine tragfähige Lösung.

Wächterfunktion: Trusted Communication Unit

Die M³-Plattform begegnet dieser Problematik mit einer neuartigen Chip-Architektur. Dabei werden Prozessoren und Beschleuniger auf dem Chip in separaten Kacheln angeordnet. Über ein Chip-Netzwerk können diese Kacheln miteinander kommunizieren. Dabei ist zwischen diesem Netzwerk und jeder einzelnen Kachel eine Wächterkomponente namens Trusted Communication Unit (TCU) geschaltet. Diese TCU ist als Hardware-Firewall dafür zuständig, nur solche Kommunikationswege zuzulassen, die explizit als erwünscht freigeschaltet wurden. Dadurch können die einzelnen Kacheln zielgerichtet miteinander kommunizieren. Unerlaubte Kommunikation, die durch einen Fehler oder Angriff induziert sein könnte, wird aber abgeblockt. Dadurch ergibt sich, ähnlich zum Mikrokernsystem, eine Chip-Architektur mit der TCU als einer gehärteten und überprüfbaren Isolationsschicht, welche die Kacheln so voreinander schützt, dass Fehler in einem Prozessor oder Beschleuniger den Rest des Systems nicht beeinflussen können. Der geringe Mehraufwand, der durch die Kommunikation über TCUs entsteht, kann in den meisten praktischen Anwendungsfällen vernachlässigt werden.

Sichere Integration und individuelle Verschaltung

In Bezug auf die genannten Spannungsfelder ermöglicht M³ damit die sichere Integration von Prozessoren und Beschleunigern, was zu hoher Energieeffizienz beiträgt. Die einzelnen Kacheln lassen sich flexibel kombinieren, so dass ein Plattform-Chip mit einem Baukasten an Prozessoren und Beschleunigern ausgestattet werden kann. Ein solcher Chip lässt sich kostengünstig in großer Stückzahl fertigen und wird folgend für eine konkrete Anwendung spezialisiert, indem nur die für den Anwendungsfall benötigten Kacheln über die TCUs miteinander verschaltet werden. Die TCUs ermöglichen dabei eine Abgrenzung von Programmbestandteilen, so dass diese auch einzeln aktualisiert werden können. Zentrale Komponenten für die Betriebssicherheit können dabei unverändert belassen werden, so dass kritische Eigenschaften überprüfbar erhalten bleiben.

Plattform-Chips auf Basis der M³-Architektur können nach Ansicht des Barkhausen Instituts damit eine Vielzahl neuer digitaler Halbleitersysteme für Medizingeräte erschließen. Die Dresdner Forschenden arbeiten in zahlreichen wissenschaftlichen Projekten daran, die M³-Architektur weiter zu verbessern. Sowohl die Software als auch die Hardware stehen anderen Forschenden und der Industrie als Open Source zur Verfügung. Der Vorteil der Architektur liegt dabei auch in ihrer hohen Fehlertoleranz. Sollte in einer Kachel ein Problem auftreten, bleibt dieses auf die betroffene Einheit beschränkt. Für die Fehlersuche muss zudem nur die relevante Kachel überprüft werden. Dieser modulare Ansatz verspricht somit, die Sicherheit und Zuverlässigkeit medizinischer Hardware sowie die Vertrauenswürdigkeit zukünftiger vernetzter Medizingeräte signifikant zu verbessern. (uh)

Per Tool-Kombi gegen Sicherheitslücken

Immun gegen Angriffe: Security für Medizingeräte

Bild: Toowongsa/stock.adobe.com

Ob gezielter Anschlag oder großangelegter Cyberangriff – vernetzte Medizingeräte müssen gegen vielfältige Angriffsarten geschützt sein. Welche Normen und Richtlinien geben Orientierung in der Entwicklung? Handreichung zu Analysemethoden, dem statischen und dynamischen Testing und dessen Kombination.

Von Royd Lüdtke
und Artur Hirsch
Verifysoft

Ohne Mikrocontroller und Softwaresteuerung kommt kein modernes, digitalisiertes Medizingerät aus. Je nach genauem medizinischen Einsatz und Kritikalität sind die Anforderungen an die Softwarequalität durchaus unterschiedlich, prinzipiell wird nach funktionaler Sicherheit (Safety) sowie der Sicherheit gegenüber Angriffen von außen (Security) beurteilt.

Die Bedeutung der funktionalen Sicherheit für in der Medizin eingesetzte Geräte ist klar. Seit der Vernetzung rückt jedoch der Bedarf an Sicherheit gegen Angriffe mehr in den Fokus. Heute kommunizieren medizinische Geräte über das Internet mit Ärzten, untereinander und auch mit anderen Institutionen. Dieses »Internet of Medical Things« (IoMT) eröffnet große Chancen, birgt aber auch große Risiken, denen Softwarehersteller durch umfangreiche Test- und Analysemethoden begegnen müssen.

Vorteile und Chancen vernetzter Medizingeräte

Ob vernetztes Ultraschallgerät, Herzschrittmacher oder Infusionspumpen – netzfähige Medizingeräte können Kosten senken sowie Lebensqualität und Überlebenschancen von Patienten drastisch erhöhen. Sie ermöglichen es Ärzten etwa, die Vitalfunktionen ihrer Patienten remote zu überwachen und Medikamentendosierungen durch Fernsteuerung anzupassen. Die Möglichkeit der Überwachung von Patienten rund um die Uhr, verbunden mit im Notfall automatisch ausgelösten Alarm- und Standortmeldungen, verkürzt überlebenswichtige Reaktionszeiten signifikant. Direkt miteinander kommunizierende Geräte können in medizinisch vertretbaren Umfang auch selbständig agieren. Wird z. B. durch eine kontinuierliche Blutzuckermessung eine drohende Unterzuckerung erkannt, so kann unverzüglich eine Meldung an eine Infusionspumpe erfolgen, die eine Glukosemenge injiziert.

Lebens- oder gesundheitsgefährdende Situationen durch Ausfall oder Fehlfunktion von medizinischen Geräten sind glücklicherweise selten, vereinzelt aber dennoch zu verzeichnen. Softwaregesteuerte Geräte sind heute vielfach in der Lage, Selbstdiagnosen durchzuführen und – sofern netzgebunden – Fehlfunktionen zu melden. Damit wird die Ausfallsicherheit erheblich verbessert.

Risiken vernetzter Medizingeräte

Mit der Gerätevernetzung wird jede individuelle Sicherheitslücke eines Geräts gefährlicher. Netzwerkschnittstellen sind aus Entwicklersicht immer als potenzielle Einfallstore für Angriffe von außen zu betrachten (**Bild 1**) – Angreifer könnten unter Ausnutzung von

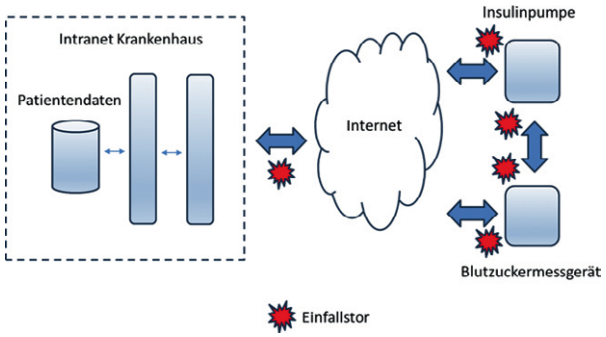


Bild 1.
Risiko vernetzter Medizingeräte.
(Bild: Verifysoft)

Sicherheitsschwachstellen die Kontrolle über ein Medizingerät erlangen – mit weitreichenden Folgen. Medizinische Geräte wurden mittelbar bereits genutzt, um in Infrastrukturen von Krankenhäusern und Gesundheitszentren einzubrechen. Bekannt geworden sind diese Einbrüche unter dem Namen »MEDJACK« (Medical Device Hijack). Ausgenutzt wurden etwa veraltete Betriebssysteme oder unsichere Programmfunktionen.

Ob persönliche kriminelle Motive oder typische Cyberverbrechen wie Ransomware-Attacken bis hin zu möglichen Terrorakten durch Manipulation vernetzter, lebenserhaltender Geräte – über MEDJACKs lassen sich hohe Sach- und Personenschäden anrichten. So können Patienten- und Personaldaten abgegriffen, weitere Geräte infiziert oder wichtige Daten böswillig verändert oder verschlüsselt werden.

Wie werden solche Angriffe in der Regel durchgeführt?

Es gibt viele Einfallstore, die ein Angreifer auszunutzen kann – oft kombinieren Angreifer mehrere Methoden.

Ein Angreifer kann in einem Netzwerk als »Man-in-the-Middle« agieren, um den Datenverkehr auszuspähen. Durch Extrahieren von Zugangsdaten und die Suche nach Schwachstellen ist es möglich, Schadcode zu injizieren. Die Ausprägungen reichen vom Zugriff aus der Distanz über Keylogger bis hin zum Sperren/Verschlüsseln von Daten oder ganzen Geräten, um diese gegen Zahlung hoher Geldbeträge wieder freizugeben – so geschehen bei zahlreichen Ransomware-Angriffen auf Einrichtungen des Gesundheitswesens.
Denial-of-service-Attacken hingegen setzen auf das Überfluten eines Datenempfängers mit einer sehr großen Menge an Datenpaketen. Dies führt zu einer eingeschränkten oder auch komplett verhinderten Funktion des Angegriffenen.

Aber auch die Software der einzelnen Medizingeräte selbst (z. B. Firmware) kann als Sprungbrett für Angriffe genutzt werden. Diese Software besteht oft aus einem Eigenentwicklungsanteil und extern entwickelten Komponenten. Um Sicherheit gegenüber Angriffen von außen zu gewährleisten, müssen Entwickler sowohl selbst erstellten Code als auch externe Softwarekomponenten auf Sicherheitslücken hin überprüfen.

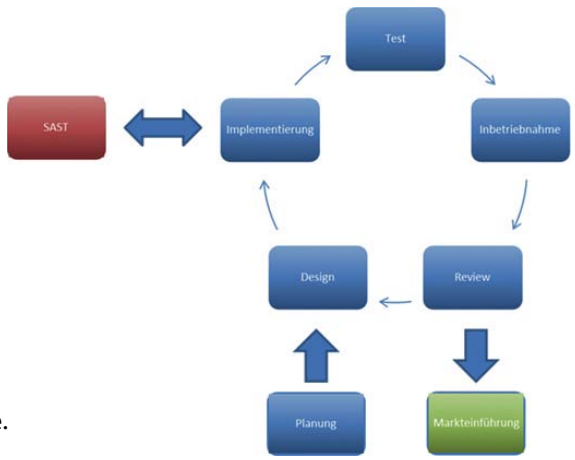


Bild 2.
SAST im Software-Lifecycle.
(Bild: Verifysoft)

Normen und Richtlinien für Softwarehersteller

Zur Vermarktung von Medizinprodukten in Europa ist die Medizinprodukteverordnung (MDR) bindend. Diese schreibt eine Risikomanagement- und Risiko-Nutzen-Analyse vor. Einen Leitfaden zum Risikomanagementprozess hinsichtlich der funktionalen Sicherheit eines Produkts bietet die ISO 14971. Nicht bindend, aber sehr hilfreich ist die AAMI TIR57 als Erweiterung der ISO 14971, um den Risikomanagementprozess auf Cybersecurity auszuweiten.

Grundsätzlich sind für den Prozess von der Produktidee bis zur Marktherausnahme die von der EU-Kommission veröffentlichten Normen IEC 62304, IEC 82304-1 und IEC 60601-1 anzuwenden. Für Medizinprodukte, die in Netzwerken betrieben werden, ist zudem die Norm IEC 80001-1 relevant. Zu erwähnen ist auch die Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union.

Statische Analyse und dynamisches Testen

Zur Gewährleistung der Softwarequalität kommen während des Softwareentwicklungsprozesses grundsätzlich zwei komplementäre Test- und Analyseverfahren zur Anwendung: Die statische Codeanalyse und das dynamische Testen.

Die statische Analyse untersucht Quellcode- und Binärdateien im Hinblick auf enthaltene kritische Fehler und Sicherheitsschwachstellen, ohne den Code ausführen zu müssen.

Die dynamische Analyse beurteilt durch Ausführen von Tests dagegen das Laufzeitverhalten der Applikation oder des Moduls. Aufgedeckt wird überwiegend funktionales Fehlverhalten, das aber durchaus auch Sicherheitsschwachstellen bedingen kann. Zum Ausführen von Tests muss bereits funktionsfähiger Programmcode vorhanden sein. Die statische Analyse hingegen ist bereits früher – begleitend zur Implementierung – einsetzbar.

Im Entwicklungszyklus wird die statische Security Analyse (SAST) je nach Entwicklungstand auch bereits auf noch nicht lauffähige Applikationsteile (z. B. Funktionen) angewandt (**Bild 2**). In dieser Phase lassen sich nach Analyse mit Tools wie CodeSonar notwendige Korrekturen im Quellcode frühzeitig und damit noch kostengünstig umsetzen.

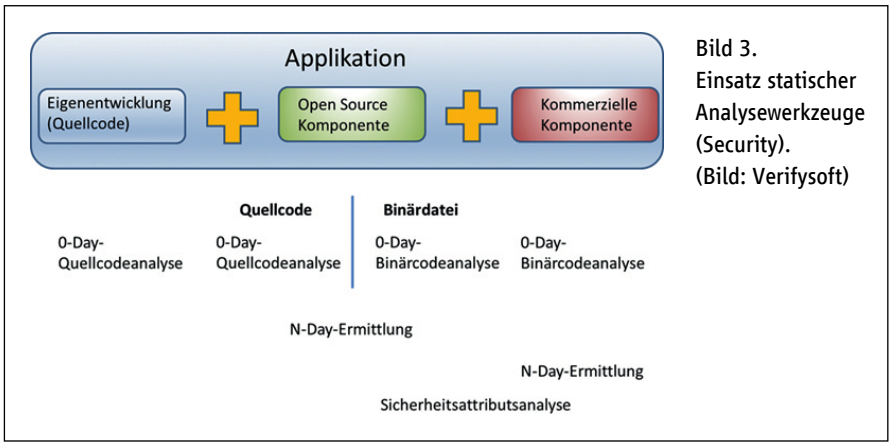


Bild 3. Einsatz statischer Analysewerkzeuge (Security). (Bild: Verifysoft)

Tools für die statische Analyse

Zur statischen Analyse stehen verschiedene Werkzeuge zur Verfügung (**Bild 3**): Einige Tools scannen den Quellcode und sind spezialisiert darauf, Schwachstellen wie Speicherüber- und -unterläufe, Format-String-Probleme, hart codierte Passwörter, geringe Verschlüsselungstiefen und eingebaute Hintertüren (Backdoors) aufzudecken. Andere Werkzeuge konzentrieren sich auf die Analyse von Binärdateien wie Bibliotheken und deren Abhängigkeiten zu eventuell weiteren eingebundenen Komponenten, um potenzielle Sicherheitslücken zu identifizieren. Insbesondere wird dabei auch nach Code-Konstrukten gesucht, die aktuell zu bekannten Sicherheitsschwachstellen geführt haben. Durch die Kombination dieser Vorgehensweisen lassen sich viele potenziell kritische Sicherheitslücken im Quellcode beheben, bevor die Software in Betrieb genommen wird.

Bei eigenentwickeltem Code empfiehlt sich die oben beschriebene Quellcodeanalyse. Das gleiche gilt für eingebundene Open-Source-Komponenten, für die der Quellcode im Zugriff steht. Man spricht hier von »0-Day-Analyse«, da damit noch unbekannte Sicherheitsschwachstellen aufgedeckt werden können. Im Hinblick auf die Open Source-Komponenten bietet sich zudem eine Überprüfung auf bekannte Sicherheitsprobleme (N-Day-Ermittlung) mittels Recherche in einschlägigen Vulnerability-Datenbanken an. Entwickler erhalten so Informationen über die Kritikalität von enthaltenen Sicherheitsschwachstellen sowie eventuell bereits vorhandene Korrekturen.

Kommerzielle Komponenten liegen zumeist nur als Binärdateien vor. Hier empfiehlt sich zunächst eine statische 0-Day-Binärcodeanalyse. Die sicherlich notwendige N-Day-Ermittlung hinsichtlich in der Binärdatei eventuell enthaltener Open Source-Komponenten ist allerdings erst durchführbar, wenn diese identifiziert sind. Das leistet die Software Composition Analysis (SCA): Dabei werden beispielsweise Zeichenketten gesucht, die auf verwendete Open-Source-Komponenten hinweisen. Analysetools wie CodeSentry ermöglichen zudem auch ohne Zugriff auf den Quellcode skalierbare Analysen. Anschließend können die Datenbanken auf bereits bekannte Schwachstellen abgefragt werden.

Grundsätzlich sollte Software, die in vernetzten Geräten zum Einsatz kommt, einer statischen »Taint Data Analyse« – einem virtuellen Penetrationstest – unterzogen werden. Man untersucht dabei, wie eingespeister Schadcode in der Applikation weitergeleitet würde und welche Funktionen davon betroffen wären. Dadurch lassen sich bereits im Vorfeld Gegenmaßnahmen treffen.

Zum Abschluss, wenn die vollständige Applikation gebaut worden ist, sollte noch eine Sicherheitsattributsanalyse durchgeführt werden. Hierbei wird überprüft, ob z. B. von der Möglichkeit, den Compiler zusätzliche Sicherheitsmechanismen in den Binärcode einbauen zu lassen, Gebrauch gemacht wurde.

Ein Muss: Die Test-Kombination

Die dynamische Analyse ist ein zur statischen Analyse komplementäres und unverzichtbares Verfahren, um die Zuverlässigkeit von Software sicherzustellen. Das dynamische Testen kann allerdings erst dann erfolgen, wenn ablauffähige Teile der Applikation (z. B. Module) vorliegen.

Im Rahmen dieser Tests wird die einwandfreie Funktionalität inklusive der für die Security relevanten Komponenten überprüft. Ein Werkzeug zur Messung der Testabdeckung stellt sicher, dass keine Tests ausgelassen wurden. Unter Einhaltung der beschriebenen Prozesse und Vorgaben zu Planung, Design, Entwicklung und Analyse von Software zum Einsatz in Medizingeräten kann ein hohes Maß an Sicherheit gewährleistet werden. (uh)

DDS-Standard für Echtzeitvernetzung ohne Single Point of Failure

Datenbus für schlaue Medizingeräte

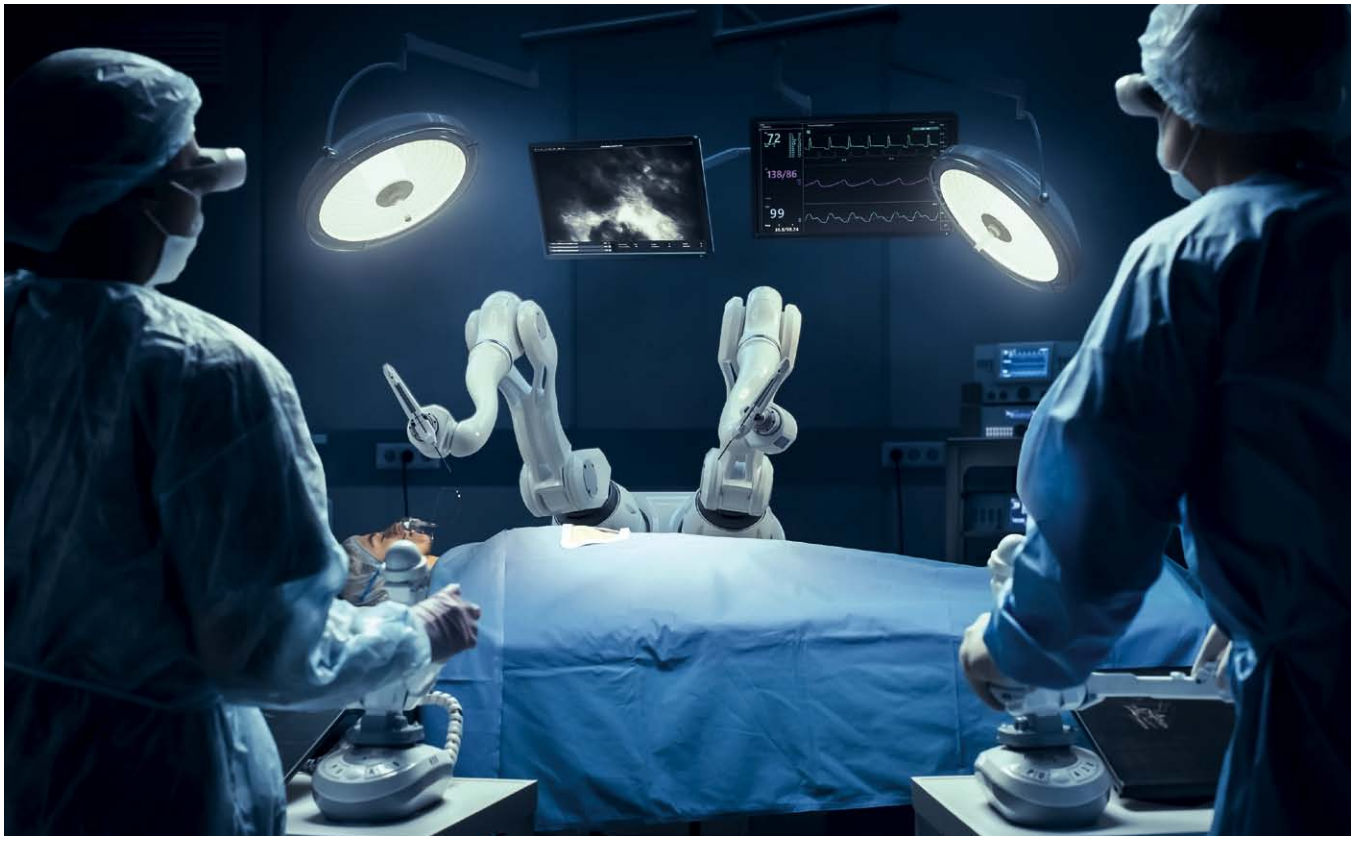


Bild: Gorodenkoff/stock.adobe.com

Die intelligente Vernetzung ist eine große Chance für die Medizin. Vernetzte Geräte, Robotik und KI verändern OP- und Klinik-Workflows im Eiltempo. Der Weltmarkt für intelligente medizinische Systeme soll sich noch dieses Jahr auf 94,2 Milliarden Dollar vervierfachen. Datenzentrierte Kommunikation ist der Schlüssel dieser Entwicklung, von RTI gibt es eine Referenzarchitektur für die medizinische Vernetzung in Echtzeit.

Darren Porras
Medical Market Manager, Real Time Innovation

Die Gesundheitssysteme sind stark gefordert: Sie müssen Kosten und Personalmangel in den Griff bekommen und gleichzeitig einer steigenden Zahl an Patienten eine hochwertige Versorgung bieten. Helfen soll dabei die moderne Technologie, der Handlungsbedarf ist klar: Medizinische Geräte müssen intelligenter und flexibler werden. Die Integration von Robotik, bildgebenden Verfahren, Sensoren und datengesteuerten Technologien ist unerlässlich für minimalinvasive und präzise Gesundheitsversorgung. Laut Studien soll sich der Weltmarkt für vernetzte medizinische Geräte von 26,5 auf 94,2 Milliarden Dollar fast vervierfachen. Die Medizintechnik muss sich also sehr schnell von isolierten Produkten und Geräten hinzu multifunktionalen, integriert-digitalen Ökosystemen wandeln.

Mit den großen Fortschritten in den Bereichen KI, Datenanalyse und Robotik müssen Medizingerätehersteller neue Systeme und Geschäftsmodelle entwickeln, die auf Software und datengesteuerten Technologien basieren. Die neuen Produkte müssen Daten aus verschiedenen Quellen und verteilten Anwendungen und Systemen integrieren und verarbeiten. Das Design muss zudem eine kontinuierliche Weiterentwicklung und Interoperabilität ermöglichen, entweder durch ein Upgrade oder durch die Veröffentlichung einer neuen Version oder eines Derivats.

Intelligenter Datenfluss und Datenzentrierung

Traditionelle Software-Kommunikationsarchitekturen arbeiten nachrichtenzentriert, die Nachrichten werden einfach zwischen den Anwendungen ausgetauscht. Eine solche Architektur (meist Punkt-zu-Punkt oder serverbasiert) ist in der Regel nicht skalierbar oder flexibel genug für zunehmend verteilte und komplexe Systeme. In einem datenzentrierten System dagegen

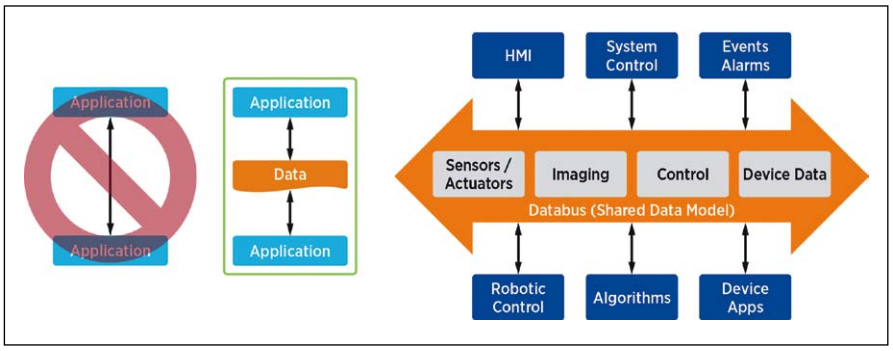


Bild 1. Mit einem datenzentrischen Datenbus können modulare Anwendungen bei Bedarf remote auf die benötigten Daten zugreifen, und zwar mit der erforderlichen Geschwindigkeit, wobei die Nachrichten von der Anwendungslogik abstrahiert werden. (Bild: RTI)

stehen die Daten im Mittelpunkt. Verteilte Anwendungen können kommen und gehen und auf Peer-to-Peer-Basis kommunizieren. Ein gemeinsames Datenmodell bildet die Grundlage für die Implementierung einer Anwendung. Eine datenzentrische Architektur abstrahiert die Kommunikation von der Anwendungslogik, so dass das Datenmodell die Kommunikationsschnittstelle darstellt. Anwendungen können von überall im System auf Daten zugreifen (**Bild 1**).

Eine datenzentrierte Kommunikationsarchitektur tauscht »Zustände« und nicht nur Nachrichten aus. Anwendungen werden über relevante Änderungen des gemeinsamen Zustands informiert, einschließlich Datenwerten, neuen Datenobjekten und der Verfügbarkeit und Aktivität anderer Anwendungen. Die Architektur ist modular und dezentral. Dies ermöglicht hohe Zuverlässigkeit, Skalierbarkeit und geringe Latenzzeiten für vernetzte medizinische Echtzeit- und intelligente Geräte. Datenzentrierte Kommunikation erleichtert auch und gerade in der Medizintechnik die Erstellung von robusten und hochverfügbaren Anwendungen. Darüber hinaus bietet das datenzentrierte Modell eine zeitliche Entkopplung von Anwendungen. Verzögerte Anwendungen müssen sich nur auf das Endergebnis konzentrieren, statt alle vergangenen Zustandsänderungen zu verarbeiten.

Intelligente Überwachung und Steuerung in Echtzeit

Mit Connext bietet RTI ein datenzentriertes Framework für die Verteilung und Verwaltung von Echtzeit-Datenströmen, welches bereits in Operationssälen und der Medizinrobotik zum Einsatz kommt. Mit dem Connext-Bus können Anwendungen und Medizingeräte als ein einziges integriertes System zusammenarbeiten und dem Gesundheitswesen unverzichtbare robuste Interoperabilität, Sicherheit und Echtzeitfunktionalität liefern. Basierend auf der Datenzentrierung bietet das Framework die Vorteile der Trennung von Anwendungen und Daten (Separation of Concerns) und ermöglicht so modulare und skalierbare Architekturen ohne Single Point of Failure.

Um klinische Applikationen zu entwickeln, die Geräte und Anwendungen integrieren, müssen diese in Echtzeit kommunizieren können. Das bedeutet, dass Reaktionszeiten im Mikro- oder Millisekundenbereich möglich sein müssen, um Tausende von Steuerungsentscheidungen pro Sekunde verarbeiten zu können. Connext ermöglicht es den Geräten, Daten direkt auf dem Datenbus zu veröffentlichen und zu subskribieren. Im Gegensatz zu einer Datenbank oder anderen Client/Server-Architekturen, die eine Anfrage- und Antwort-Protokollstruktur erfordern, ermöglicht Connext eine Geräte-

DATA DISTRIBUTION SERVICE

DDS ist ein datenzentrierter Kommunikationsstandard, der von der OMG gepflegt wird. Die Infrastruktur abstrahiert Nachrichtenfunktionen und Sender-Empfänger-Abhängigkeiten von der Anwendungslogik und vereinfacht so die Systementwicklung und die Weiterentwicklung vernetzter Anwendungen. Softwareentwickler können sich somit auf die Anwendungsentwicklung konzentrieren (**Bild 2**). DDS ist flexibel und funktional. Der QoS-Mechanismus bietet Lösungen für häufig auftretende Kommunikationsprobleme. Die Technologie ermöglicht die gemeinsame Nutzung verschiedener Datentypen mit der erforderlichen Datenrate. DDS formalisiert das datenzentrierte Publish/Subscribe-Kommunikationsparadigma, indem es eine standardisierte Schnittstelle und die erforderlichen Protokolle für die benötigte Funktionalität bereitstellt. (**Bild 3**).

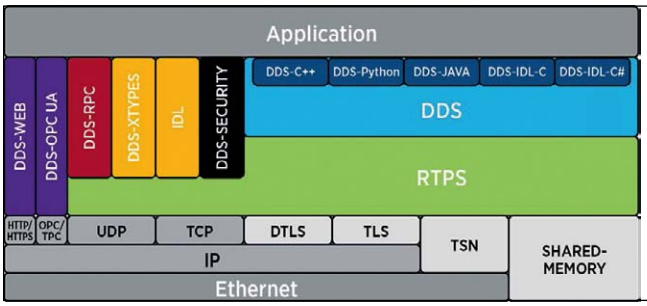


Bild 2. Aufbau einer DDS-basierten und auf Echtzeitkommunikation ausgelegten Architektur. (Bild: RTI)

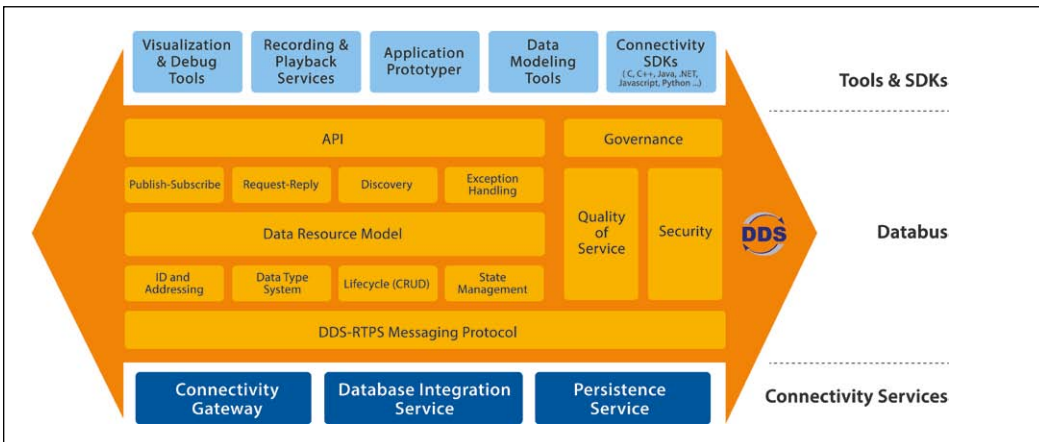


Bild 3. RTI Connext Connectivity Framework. (Bild: RTI)

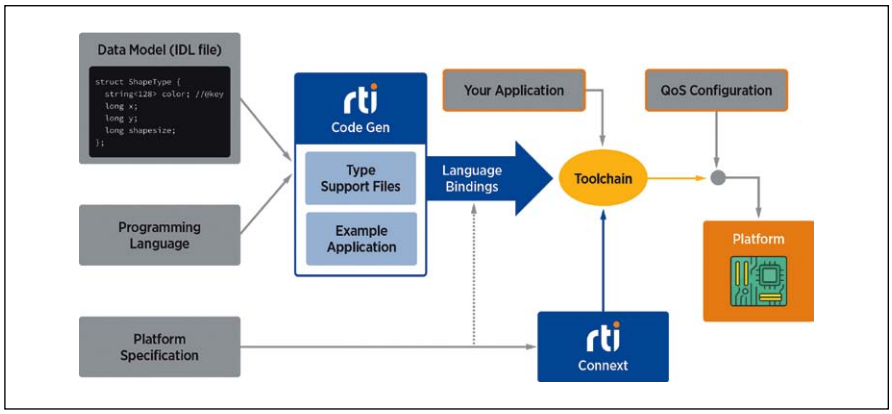


Bild 4. Anwendungsentwicklung mit RTI Connext. (Bild: RTI)

steuerung in Echtzeit indem die Daten selbst zur Nachricht werden. Das DDS-basierte Datenmodell verteilt die Echtzeitdatenmuster zum richtigen Zeitpunkt an die abonnierten Endpunkte.

Entwicklungstool für Medizingeräte

Die Connext-Entwicklungstools von RTI sind ein modernes Werkzeug für Software-Teams, die an Medizingeräten arbeiten. Die Admin-Konsole bietet eine Echtzeitansicht aller Endpunkte, in der Details nach Thema oder Endpunkt aufgeschlüsselt werden können. Mit Hilfe der Datenvisualisierung können mehrere Werte aus mehreren Themen interaktiv dargestellt und grafisch geteilt werden. Diese Funktion eignet sich für die Fehlersuche im System, zur Aufzeichnung eines bekannten, guten Zustands oder für die Entwicklung eines verbesserten Anwendungsalgorithmus. Mit dem Connext Recording and Playback Service lassen sich Datenströme in einer Datenbank speichern. Die Daten lassen sich modifizieren, um Testfälle zu erstellen und (über den Wiedergabedienst) je nach Bedarf schneller oder langsamer wiedergegeben werden, um das System für Funktionstests, Validierung, Lasttests usw. zu überprüfen.

Der Web Integration Service bietet sowohl eine REST- als auch eine WebSocket-Schnittstelle zu jedem Connext-Datenbus und ermöglicht so die Anbindung an mobile Geräte und/oder Webseiten mit einem sehr geringem Programmieraufwand. Der Connext Code Generator erfasst Datentypbeschreibungen in IDL (oder XML) und generiert funktionalen Serialisierungscode für die Zielsprache und -plattform. Der generierte Code implementiert das RTPS-Protokoll, so dass sich die Entwickler auf die anwendungsspezifische Programmierung konzentrieren können – die Toolbox übernimmt das »Klempnern«. Connext ermöglicht damit offene Architekturen für den Datenfluss über interne und externe Schnittstellen. Für Entwickler von medizinischen Systemen bietet der Connext-Datenbus eine effektive Lösung für die traditionellen Herausforderungen der Datenkonnektivität, der Plug-and-Play-Interoperabilität, der Echtzeitanalyse und der feingranularen Sicherheit, um die Vision von vollständig automatisierten IoMT-basierten Systemen zu verwirklichen und wirklich transformative Medizinsysteme bereitzustellen (**Bild 4**).

Cybersicherheit für medizinische Vernetzung

Obwohl sichere Kommunikation nur ein Teil einer insgesamt sicheren Gerätearchitektur ist, unterstreichen die jüngsten FDA-Richtlinien zur Cybersicherheit die Notwendigkeit für Medizingerätehersteller, die Sicherheitsrisiken von Kommunikationsschnittstellen im gesamten Geräteökosystem zu bewerten. Um einige dieser Bedenken auszuräumen, ermöglicht es Connext Secure, die Zugriffskontrolle (niedrigste Autorisierung) auf Daten in Bewegung zu konfigurieren, wobei es Anwendungsfälle und/oder Betriebsumgebungen der Datenströme berücksichtigt. Je nach Rolle und Thema ist die feingranulare Sicherheit von Datenströmen einstellbar, was den vollständigen Schutz kritischer Daten gewährleistet. Die dezentrale Architektur des Connext Frameworks und die QoS-Kommunikationsmuster stellen die Verfügbarkeit des Datenzugriffs sicher und ermöglichen robuste Datenströme. Ebenfalls verfügbar sind Plug-ins für Authentifizierung, Kryptografie, Zugriffskontrolle, Data Tagging und Security Logging. Weil die QoS den Sicherheitsstatus jeder DDS-Einheit verwaltet, sind keine Code-Änderungen erforderlich (**Bild 5**).

Echtzeitintelligenz im IoMT

Eine kombinierte Überwachung, Optimierung und Autonomie könnte im Gesundheitswesen bedeuten, auf der Überwachungsebene kontinuierlich Daten aus diversen Datenquellen zu sammeln, um den Zustand von Patienten und Geräten zu erfassen. Medizinsysteme könnten so Automatisierung, Kontrolle und klinische Entscheidungsunterstützung bieten, um etwa die Alarmmüdigkeit auf Intensiv- oder Pflegestationen zu beseitigen. Bei vollständiger Automatisierung könnten Daten von einem Gerät erfasst und an ein weiteres Gerät übertragen werden, das dann mithilfe von maschinellem Lernen oder KI eine klinische Entscheidung bestätigt und die empfohlene Behandlung einleitet. Derartige Fortschritte sind in der chirurgischen Robotik, der Bildgebung und bei minimalinvasiven, diagnostischen und therapeutischen Anwendungen bereits in der Entwicklung und Praxis. Nicht nur, aber speziell in der Medizintechnik beschleunigt sich die technologische Entwicklung rasant. Intelligente und vernetzte Geräte in Verbindung mit Edge Computing werden die Workflows am Point-of-Care umkrempeln. Eine wichtige Basis für diese digitale Transformation sind die Echtzeitarchitekturen und Datenbusse der intelligenten und vernetzten Systeme. (uh)

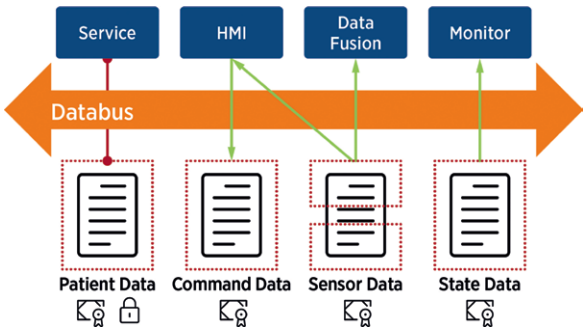


Bild 5. Datenzentrierte Cyber-Sicherheit ermöglicht die Entwicklung von Systemen zur Beschränkung der Zugriffskontrolle (z. B. Authentifizierung, Verschlüsselung) auf Daten in Bewegung auf der Grundlage des Prinzips der geringsten Rechte. (Bild: RTI)

Exklusiv-Interview ams Osram

»Wir brauchen KI, um das Photon-Counting-Potenzial voll auszuschöpfen«

Für Computertomografen ist Photon Counting ein Quantensprung. Dr. Erik Greger von ams Osram gibt Einblicke in die bahnbrechende Detektortechnik, zeigt wie KI die Radiodiagnostik neu kalibriert und mit welchen Röntgen- und CT-Innovationen der ASIC-Spezialist Markt- und Technologieführer werden will.

Von Ute Häußler

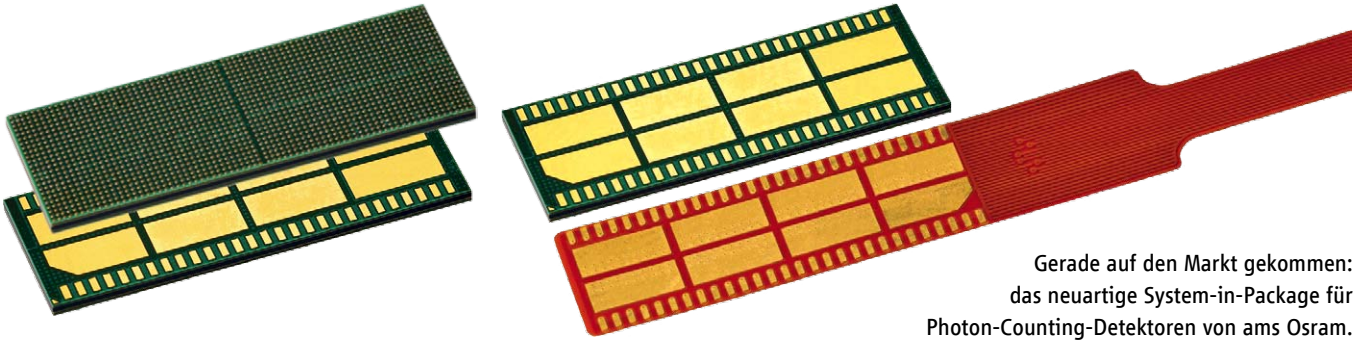
Herr Dr. Greger, wie wichtig ist Medizintechnik für ams Osram und die Division CMOS und ASICs?
Dr. Erik Greger: Die Medizintechnik ist neben Automotive und Industrial einer der wichtigsten Märkte für ams Osram, speziell aber auch für die Division CMOS und ASICs und die Business Line Mixed Signal Products (MSP). Es ist ein Wachstumsmarkt und im Gegensatz zum Consumer-Geschäft ein sehr stabiler Markt. Health ist ein Megatrend unserer Zeit, sowohl in der zentralen Gesundheitsversorgung als auch mit Wearables für den Alltag. Ein gesundes Leben, Fitness – viele Menschen wollen heutzutage alles tracken – diese Entwicklung zahlt auf unsere Sensoren und Halbleiterprodukte immens ein.

Bilder: Cristiano; Yvonne Bogdanski/stock.adobe.com

Welches sind die wichtigsten Medtech-Komponenten und für welche Applikationen?
In unserem Team sind das Detektoren oder ASICs für die Computertomografie und Röntgen-Anwendungen. Die Kollegen der Business Line Advanced Analog Solutions beschäftigen sich mit den Naneye-Mini-Kameramodulen und passenden LEDs für Einmalendoskope. Unser »Vital Signs«-Bereich beschäftigt sich an der Grenze von Medizin und Consumer-Electronics mit Sensoren, Fotodioden sowie Multichips für die Vitalzeichenmessung in Wearables und weiteren Medizingeräten. Und dann haben wir auch noch die Spektroskopie mit hochakkuraten Spektralfiltern und Optical Force Sensing für hygienische Bedienelemente an Medizingeräten.

Sie sind quasi der Chefradiologe bei ams Osram?
lacht Ich leite die Business Line MSP, die Produktlinie für die Radiologie ist eine davon. Es ist ein faszinierender Wachstumsmarkt, und es macht viel Freude zu sehen, wie unsere Ingenieure und Entwickler mit viel Know-how und neuen Ideen die Technologie und damit die Diagnostik für Ärzte und Patienten wirklich nach vorn bringen.

ams Osram will marktführend bei Radiologie-Komponenten werden. Wo stehen Sie derzeit bei Umsatz und Marktanteil?
Die Medizinische Bildgebung ist ein überschaubarer Markt, es gibt nicht so viele Player. Im CT-Bereich arbeiten wir bereits mit acht der Top-10-OEMs zusammen. Als Zulieferer und Entwicklungspartner sind wir aus meiner Sicht sehr gut positioniert. Unser klares Ziel ist, in der Radiologie die Nummer eins zu werden. Ein Aspekt davon ist Innovation: Wir wollen den technologischen Benchmark setzen und ein richtungsweisendes Portfolio sowohl für die Computertomografie als auch fürs Röntgen anbieten.



Gerade auf den Markt gekommen: das neuartige System-in-Package für Photon-Counting-Detektoren von ams Osram.

Was bedeutet Innovation für Sie bezogen auf Technologien für die Radiologie?
Mit »Photon Counting« steht die Computertomografie vor einer disruptiven Veränderung. Das ist wie der Wandel von der Schwarz-Weiß-Röhre zum Farbfernsehen. In die neuen Photon-Counting-Detektoren haben wir sehr viel investiert, das ist ein sehr wichtiger Aspekt.
Für Röntgengeräte sprechen wir von Fortschritten hinsichtlich Geschwindigkeit (Frames pro Sekunde) und Strahlungsdosis, die zum Beispiel Ärzte während Operationen in Echtzeit zu unterstützen, wo sie die Nadel oder das Skalpell setzen müssen. Für diese OP-Applikationen brauchen sie hochsensitive Detektoren, die in der Lage sind, auch geringe Strahlungsquellen hochauflösend zu detektieren und damit die Strahlendosis gering zu halten.

Grundlegend verbessert sich in beiden Fällen die Bildqualität, und die Patienten werden weniger Strahlung ausgesetzt. Beim Photon Counting kommt hinzu, dass CT-Geräte in die Lage versetzt werden, verschiedenen Gewebeelementen über sogenannte Energy Buckets Farben zuzuordnen. Diese Spektralanalyse ist ein wesentliches Merkmal der PCCT-Technologie.

Welche Märkte will ams Osram insbesondere ansprechen?
Wir verstehen uns auch in der Radiologie als globaler Player. Wir arbeiten mit allen namhaften Medical-OEMs zusammen, nicht nur in Europa und den USA. Hinsichtlich der Marktchancen: Studien sagen für die Regionen USA und EMEA weiter rund 6 Prozent jährliches Wachstum voraus; China und Indien werden oft als die am schnellsten wachsenden Märkte für medizinische Geräte genannt. Auch ein weiterer Megatrend weist die Richtung: Die medizinische Versorgung muss in abgelegene Weltregionen vordringen. Viele Schwellenländer statten über spezielle Gesundheitsprogramme Kliniken mit CT- und Röntgengeräten aus. An all diesen Märkten partizipieren wir über unsere Kunden.

Die großen Hersteller, darunter Siemens Healthineers, entwickeln Sensoren und Detektoren selbst. Konzentrieren Sie sich ergo auf OEMs ohne eigene Entwicklung?
Wir arbeiten – in unterschiedlichen Ausprägungen – mit allen namhaften Herstellern zusammen. Unsere Kernkompetenz über die Wertschöpfungskette ist das ASIC-Design. Auf den hochsensitiven Low Power- und Analog-Digital-Wandlern wird auch künftig unser Fokus liegen. Andererseits sehen wir bei unseren Medizintechnikkunden einen Shift hin zu IoT, KI sowie Softwarefeatures. Das ist auch für uns eine Chance, uns in der Wertschöpfungskette weiter nach oben zu bewegen. So bieten wir zum ASIC-Design bereits Module an, teilweise mit Szintillator. Das ist je nach Kunde sehr unterschiedlich – wir sehen auf jeden Fall den Trend und bleiben offen.

Ein richtungsweisendes Beispiel für diese Entwicklung ist das Photon Counting: Die bereits genannten Energy Buckets generieren wahnsinnig viele Daten; mehr Daten, als sich je ein Radiologe ansehen kann. Der Trend zu KI und der Softwarezentrierung bei den OEMs kommt also nicht von ungefähr. Der Enduser im Krankenhaus hat allein aus Kostengründen nur begrenzt Zeit für einen Patienten. Um das Potenzial der neuen Technologie voll auszuschöpfen, werden wir KI brauchen. Auch der Trend zu Remote-Work und Remote-Wartung zahlt auf den Software-Shift in der Radiologie ein. Das eröffnet uns bei ams Osram viele neue Chancen.

Wo liegt für Sie größeres Potenzial: im CT oder im Röntgen?
Das ist eine schwierige Frage. In den letzten drei Jahren hatten wir mit dem Photon Counting mehr Fokus auf die CT-Technik gelegt, wir haben da viel investiert. Aber aktuell sehen wir auch viele Möglichkeiten bei Röntgenanwendungen – ich denke, dass wir künftig wieder mehr im Röntgensegment machen werden. Nicht zuletzt auch über die Medizin hinaus.

Sie meinen industrielles Röntgen?
Industrielles Röntgen spielt eine große Rolle, aber auch die Security. Wenn Sie Glück haben, steht an der Sicherheitskontrolle am Flughafen einer der neuen CT-Röntgenscanner, und Sie kommen schneller durch. Die Industrie und die Security eröffnen uns neue Betätigungsfelder und unterstreichen, dass wir wachsen und in die Breite gehen wollen.

Wenn wir in der Medizin bleiben: Wo liegen die technischen Vorteile Ihrer PCCT-Detektoren?
Aus meiner Sicht haben wir eine sehr elegante Lösung entwickelt. Gegenüber dem Mitbewerb bieten wir ein Plug-and-play-Produkt, und zwar über Produktgenerationen hinweg. Wenn ein OEM auf die nächste Detektorgeneration wechseln will, muss er sein System nicht ändern. Das erspart unseren Kunden sehr, sehr viel Aufwand. Zum anderen haben wir unsere Photon-Counting-Lösung in ein spezielles Package gepackt – ein sogenanntes Buttable System-in-Package (BSiP).

Welche Vorteile bringt das in der Entwicklung?
Ein CT-Detektor ist ein Stückwerk. Sie haben mehrere Sensor-Chips, die Sie zu einer Detektor-Fläche zusammenstecken. Ideal dafür sind Four-Side-Buttable-Sensoren, die von allen vier Seiten ansetzbar sind, deswegen Buttable. Genauer gesagt haben wir ein Four-Side-Buttable-System-in-Package, in das die ICs und einige andere Komponenten vollständig integriert sind. Das macht es sehr robust und sehr einfach zu verarbeiten und zu handhaben. Viele medizinische ASICs werden auch hier in Premstätten gefertigt (bei Graz, Österreich, Anm. d. Red.).

Auch das Package?
Eine eigene Packaging-Linie haben wir nicht, dafür haben wir unsere OSAT-Partner (outsourced semiconductor assembly and test, Anm. d. Red.), wie alle anderen auch. Der Zug für Packaging-Linien in Europa

ist leider abgefahren. Aber alles Silizium kommt hier aus der Fabrik nebenan. Mit Ausnahme des Photon Countings, da kommt es derzeit noch von einem Partner.

Wie sind die weiteren Pläne für die PCCT-Detektoren?
Die Produkt-Roadmap steht über die erste Generation hinaus. Wir wissen, was wir in der zweiten, in der dritten Generation machen wollen. Dabei stehen zwei, drei Themen im Vordergrund.

Das erste ist, dass am Ende der ASIC mit dem Cadmiumtellurid (CdTe, auf diesem Kristall basiert das Photon-Counting , Anm. d. Red.) zusammenspielen muss, das das Röntgenlicht in abzählbare Elektronen umwandelt. Wir arbeiten dazu mit allen namhaften Anbietern zusammen, dieses Thema müssen alle OEMs gelöst kriegen. Zum zweiten ist »Low Power« wichtig. Die Pixel sind beim Photon Counting wesentlich kleiner als bei konventionellen CT-Scannern, damit muss auch die Power-Fläche pro Pixel kleiner werden – OEMs brauchen also zwingend eine Low-Power-Lösung. Das dritte Thema sind Features. Die Photon-Counting-Technologie wird die Computertomografie wahrscheinlich über die nächsten 25, 30 Jahre tragen. Das heißt, während der nächsten Dekaden werden zusätzliche Funktionen in die Systeme Einzug halten. Alles, was jetzt auf dem Markt platziert wird, sind Grundfeatures. Wir haben bereits viele Ideen für solche, das Photon-Counting verfeinernden Add-ons.

Sie machen die Leserinnen und Leser neugierig.
Wir sprechen noch nicht konkreter darüber. Was ich aber sagen kann: Für die medizinische Diagnostik sind Artefakte und deren Herkunft ein kritisches Thema. Beim Photon Counting etwa wird über das Cadmiumtellurid Röntgenlicht in ein Elektron-Loch-Paar umgewandelt, das Sie dann detektieren. Wenn ein Arzt auf dem daraus resultierenden Bild einen weißen Punkt sieht, muss er sicher sein können, dass dieser Punkt kein Artefakt ist.

Dr. Erik Greger leitet den Bereich Mixed Signal Products bei ams Osram.

Deshalb müssen die Hersteller ihre Designs intensiv testen: Solche Artefakte können vom Chipdesign kommen, vom Cadmiumtellurid oder auch aus unterschiedlichen Architekturen und Materialien entstehen. Das ist ein sehr spannendes Thema, weshalb wir auch sehr viel Wert auf unser Systemverständnis und System-Know-how legen. Wir haben sehr geschätzte Ingenieure im Haus, die mit unseren Kunden diese Fragen diskutieren und letzten Endes auch lösen.

Vielen Dank für den Ausblick. Wie sieht für Sie die Medizin der Zukunft aus?
Oh, ich glaube Science-Fiction-Filme sind gar mehr so weit weg von der Wirklichkeit. Um beim Anfangsbeispiel des Fernsehens zu bleiben: In meiner Kindheit hatten wir ein klobiges Schwarz-Weiß-Röhrengerät im Wohnzimmer, jetzt ist es ein sehr dünner Super-Ultra-High-Definition-TV – alles innerhalb von ein paar Jahrzehnten. Wenn Sie die Fortschritte in der Medizin über die letzten 10, 20 Jahre betrachten, zum Beispiel in der Krebstherapie, rechne ich in den nächsten Jahren und Jahrzehnten mit unglaublichen Fortschritten.

Gerade die Computertomografie liefert heute schon atemberaubende Bilder, denken Sie nur an die komplexe Physik dahinter und die Präzision. Mit der KI-gestützten Bildverarbeitung werden die Diagnostik, die Prävention und auch die OP-Qualität noch mal einen riesigen Sprung nach vorn machen – wir werden weitere Meilensteine in der Medizin erleben. Und aus meiner Sicht, das sage ich auch meinem Team ganz häufig, ist das ein wirklich guter Purpose. Jeder von uns weiß, warum er morgens aufsteht – am Ende arbeiten wir hier für eine bessere Welt und die Gesundheit von uns allen.

Ein perfektes Schlusswort, vielen Dank für das Gespräch!

Cybersecurity für Medizingeräte

Schwachstellen vor den Hackern finden

Die digitale Vernetzung von Medizingeräten verbessert die Patientenversorgung, macht sie jedoch auch anfälliger für Cyberattacken. Wie können Hersteller und Inverkehrbringer frühzeitig Risiken identifizieren? Ein Blick auf die Rolle von »Common Vulnerabilities and Exposures« und aktuelle regulatorische Anforderungen.

Von Dr. Joachim Wilke
Cyber-Security-Experte Healthcare bei ITK Engineering

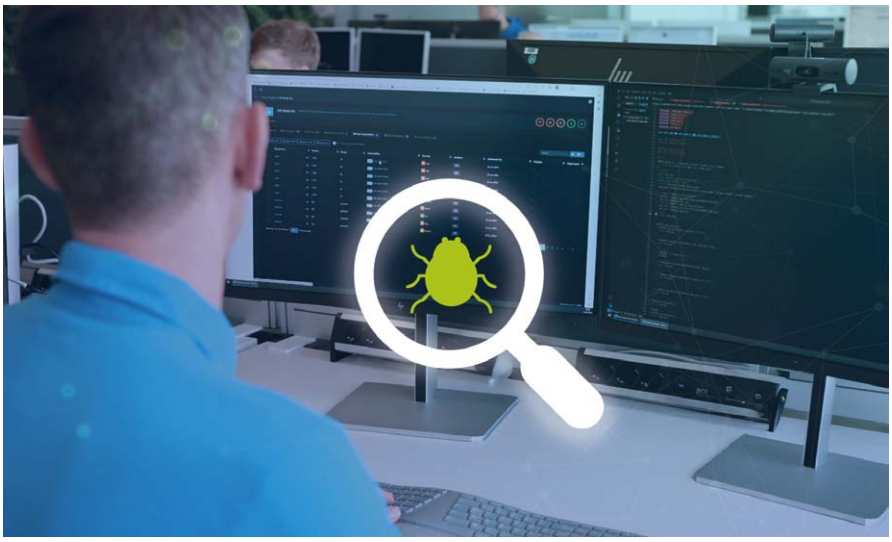


Bild 1. Effizientes Schwachstellenmanagement ist in der Entwicklung von Medizinprodukten essenziell (Bild: ITK Engineering)

Cyberangriffe auf Medizingeräte in Krankenhäusern und im häuslichen Umfeld bedrohen nicht nur sensible Patientendaten, sondern gefährden auch die Sicherheit von Patienten sowie die Funktionalität der medizinischen Geräte.

Bekannte Schwachstellen

Sogenannte »Common Vulnerabilities and Exposures« (CVEs) spielen im Kampf gegen die Bedrohungen eine zentrale Rolle. Für Hersteller und Inverkehrbringer von vernetzten Medizingeräten ist es essenziell, diese Risiken frühzeitig zu identifizieren, zu bewerten und zu beheben. Welche Bedeutung haben CVEs, wie werden sie bewertet, und wo liegen regulatorische Vorgaben?

Transparenz und Nachvollziehbarkeit sind Pflicht

Ein effektives Schwachstellenmanagement ist in der modernen Medizintechnik unverzichtbar. CVEs können als identifizierte Schwachstellen in Software und Hardware schwerwiegende Risiken wie Datenlecks oder Manipulationen verursachen. Regulierungsbehörden wie die Europäische Union und die US-amerikanische Food and Drug Administration (FDA) setzen hier klare Richtlinien. Sie fordern regelmäßige Risikoanalysen und ein dokumentiertes Schwachstellenmanagement ein.

Die Medical Device Regulation (MDR) der EU und Normen wie die IEC 81001-5-1 verpflichten Hersteller dazu, CVE-Scans – also Prozesse, die Systeme auf bekannte Schwachstellen überprüfen – fest in ihre Vorgänge zu integrieren und Berichte mit betroffenen Komponenten, Kritikalität und getroffenen Maßnahmen zu generieren. Diese Analysen sind entscheidend, um Sicherheitsrisiken frühzeitig zu erkennen. Darüber hinaus müssen alle Entscheidungen nachvollziehbar dokumentiert werden. Dies hilft, Haftungsrisiken zu minimieren und die Anforderungen von Auditoren zu erfüllen.

Software Bill of Materials

Um einen CVE-Scan durchzuführen, benötigt man eine Software Bill of Materials (S-BOM). Sie enthält alle Softwarekomponenten, aus denen das zu betrachtende System besteht, und muss oft manuell gepflegt werden. Tools können sowohl bei der Erstellung von S-BOMs als auch beim Scannen durch Automatisierung unterstützen. Lediglich die anschließende Bewertung der entdeckten Schwachstellen erfordert gründliche Handarbeit.

CVE-Scanning in der Praxis

Um die praktische Anwendung des CVE-Managements zu veranschaulichen, ein fiktives Fallbeispiel:

PRAXISTIPP

Die Implementierung eines detaillierten Audit-Logs durch ein geeignetes Tool ermöglicht die lückenlose Nachverfolgung aller Entscheidungen und Statusänderungen. Diese detaillierte Dokumentation dient in jedem Audit als wertvolle Informationsquelle und unterstreicht die Sorgfalt und Professionalität des Herstellers im Umgang mit Sicherheitsrisiken.

Dr. Joachim Wilke

Ausgangssituation: Initialer CVE-Scan und Bewertung

Ein Medizinproduktehersteller implementiert ein robustes Sicherheitsmanagement für seine Software. Nach sorgfältiger Erstellung einer detaillierten S-BOM, die zehn Third-Party-Komponenten umfasst, führt das Sicherheitsteam einen initialen CVE-Scan durch. Das eingesetzte Tool identifiziert 75 potenzielle Schwachstellen.

Die Sicherheitsexperten des Unternehmens analysieren jedes einzelne CVE-Ticket gründlich. Interessanterweise erweist sich keine der identifizierten Schwachstellen als relevant für das spezifische Medizinprodukt. Alle CVEs werden mit dem Status »Not Affected« gekennzeichnet, wobei jede Entscheidung sorgfältig dokumentiert wird. Die Ergebnisse werden in eine maschinenlesbare CycloneDX/VEX-Datei exportiert – ein Format, das zunehmend von Zulassungsbehörden wie der FDA eingefordert wird.

Post-Market-Phase: Proaktives Schwachstellenmanagement

Nach der erfolgreichen Markteinführung implementiert der Hersteller einen automatisierten wöchentlichen CVE-Scan. Diese proaktive Vorgehensweise zahlt sich aus: Zwei Monate später werden zwei neue CVEs für die verwendete OpenSSL-Bibliothek entdeckt. Die Sicherheitsexperten reagieren umgehend:

- CVE-1 wird als »Not Affected« eingestuft, da die Schwachstelle nur in einer Konfiguration auftritt, die im Produkt nicht verwendet wird.
- CVE-2 hingegen betrifft eine Funktion, die im Produkt tatsächlich genutzt wird und erhält den Status »Exploitable«.

Bereits am nächsten Tag evaluiert das Entwicklungsteam zwei Optionen zur Behebung von CVE-2:

- 1) Ein umfassendes Update der OpenSSL-Bibliothek, das jedoch weitreichende Softwareänderungen und umfangreiche Tests erfordern würde.
- 2) Die Implementierung eines offiziellen Patches, der nur wenige Code-Zeilen betrifft.

Nach sorgfältiger Abwägung fällt die Entscheidung auf Option 2: Der Patch wird innerhalb einer Woche integriert und durch gezielte Delta-Tests validiert. Anschließend wird das Patch-Release freigegeben. Der gesamte Prozess – von der CVE-Identifikation bis zur Patch-Implementierung – wird lückenlos dokumentiert und in der Medizinprodukte-Akte festgehalten. Der Status des CVE-Tickets wird final auf »Resolved« gesetzt.

Ergebnis: Strukturiertes CVE-Management

Der Ansatz schafft ein effizientes CVE-Managementsystem, das schnelle Reaktionen auf Sicherheitsrisiken ermöglicht. CycloneDX/VEX-Dateien sorgen für eine transparente, maschinenlesbare Dokumentation – ein entscheidender Vorteil bei regulatorischen Audits.

Proaktives Schwachstellenmanagement

CVE-Management steigert die Produktsicherheit und sichert effizient die regulatorische Compliance – essenziell für Medizinproduktehersteller in einer stark vernetzten Medizintechnikwelt.

Hersteller sollten CVE-Scans bereits während der Entwicklungsphase berücksichtigen und Softwarekomponenten möglichst früh aktualisieren. Dies hilft, den Aufwand der zu prüfenden und zu bewertenden CVEs zu minimieren – ein Zeitaufwand, der in der Pflege und Weiterentwicklung der eigentlichen Software definitiv besser investiert ist. (uh)

IMPRESSUM

Director Content Electronics: Dr. Ingo Kuss
Redaktionsteam: Heinz Arnold (ha/1253), Caspar Grote, Produktmanager Events (cg/1368), Engelbert Hopf, Chefreporter (eg/1320), Ute Häußler, Ltd. Red. (uh/1369), Irina Hübner (ih/1339), Andreas Knoll, Ltd. Red. (ak/1319), Dr. Ingo Kuss, Chefredakteur, verantwortlich für den Inhalt im Sinne des Presserechts (ku/1324), Corinna Puhlmann-Hespen (cp/1316), Corinne Schindlbeck, Ltd. Red. (sc/1311), Iris Stroh, Ltd. Red. (st/1326), Nicole Wörner (nw/1325), Karin Zühlke, Ltd. Red. (zü/1329)
Die Ressortverteilung entnehmen Sie bitte der Internetseite elektroniknet.de/electronics-redaktion
Layoutteam: Wolfgang Bachmaier (Ltg.), Alexander Zach
Redaktionsassistenz: Alexandra Chromy (ac/1317)
So erreichen Sie die Redaktion: Tel.: 089 25556-1317, redaktion@elektronik.de

Sales Director Electronics: Carolin Schlüter (1570)
Sales Director New Electronics: Christian Stadler (1375)
Regional Sales Managers: Burkhard Bock (1305), Emilia Dietrich (1574), Martina Greulich (1576),
Anzeigenassistenz: Rosi Böhm (1307)
Anzeigenverwaltung und Disposition: Jeanette Blaukat (1014), Stefan Buchner (Ltg., 1481)
Auslandsrepräsentanz (Foreign Representation):
USA: Véronique Lamarque, E&Tech Media, llc, 80 Kendrick Street, Brighton, MA 02135, Phone/Fax: +1 860-536-6677, E-Mail: veroniquelamarque@gmail.com, Skype: E&Tech Media
Anzeigenpreise: Es gilt die Anzeigenpreisliste Nr. 60 vom 1. Januar 2025
So erreichen Sie die Anzeigenabteilung: Tel.: 089 25556-1376
media@elektronik.de, www.elektroniknet.de/media

Vertrieb: Robin Beilicke (1340, rbeilicke@componeers.net)
Bestell- und Abonnement-Service: Componeers GmbH (ehemals WEKA Fachmedien GmbH), c/o Zenit Pressevertrieb GmbH, Postfach 810640, 70523 Stuttgart, Tel.: 0711 82651-210, Fax: 0711 82651-333, abo@componeers.net
Organschaft: Die Elektronik ist Organ der VDE/VDI-Gesellschaft Mikroelektronik, Mikrosystem- und Feinwerktechnik (GMM). Die Mitglieder der GMM erhalten die Elektronik im Rahmen ihrer Mitgliedschaft.
Erscheinungsweise: 26 Ausgaben

Jahresabonnement Print Inland	199,00 €
Jahresabonnement Print Ausland	221,10 € inkl. der aktuellen MwSt.
Einzelausgabe Print	10,00 € inkl. der aktuellen MwSt., zzgl. 3,00 Euro Versandkosten
Jahresbezug digitales E-Paper	70,00 € inkl. der aktuellen MwSt., ohne Versandkosten (Inland/Ausland)
Einzelausgabe digitales E-Paper	3,99 € inkl. der aktuellen MwSt., ohne Versandkosten (Inland/Ausland)

74. Jahrgang, ISSN 0013-5658, Vertriebskennzeichen ZKZ 2594

Druck: Vogel Druck und Medienservice GmbH, Leibnizstr 5, 97204 Höchberg, auch Anschrift für Beihefter und Beilagen.

Geschäftsführer: Matthäus Hose

Anschrift für Verlag, Redaktion, Vertrieb, Anzeigenverwaltung und alle Verantwortlichen:
Componeers GmbH, Richard-Reitzner-Allee 2, 85540 Haar
Tel. 089 25556-1000, www.componeers.net
Telefon-Durchwahl im Verlag: Sie wählen 089 25556 und dann die Nummer, die in Klammern hinter dem jeweiligen Namen angegeben ist.

WISSEN, WAS ZÄHLT
Geprüfte Auflage
Klare Basis für den Werbemarkt

Mitglied der Informationsgemeinschaft zur Feststellung der Verbreitung von Werbeträgern e.V. (IVW), Bad Godesberg

INSERENTEN

Elektronik medical

Dieser Ausgabe liegt eine Beilage der RCT Reichelt Chemietechnik GmbH & Co. bei.
Wir bitten freundlich um Beachtung!