konplan

Security Herausforderung in der Entwicklung von mechatronischen Systemen

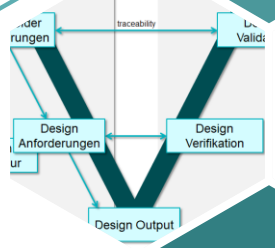
Ivo Locher

Program Manager

konplan ag

7. März 2023

IoT Security



Ivo Locher

Program Manager at konplan

- (Medical) Mobile Apps
- Cybersecurity Mandate
- Verschiedene mechatronische Entwicklungsprojekte (Wearable, Injektor, Apex locator)

Schwerpunkte:

Projektmanagement

Internet of Medical Things

Cybersecurity in der Entwicklung

Technische Schwerpunkte:

Systems Engineering, Methodiken, Risikomanagement

Elektronik, Signalverarbeitung

konplan

developing together

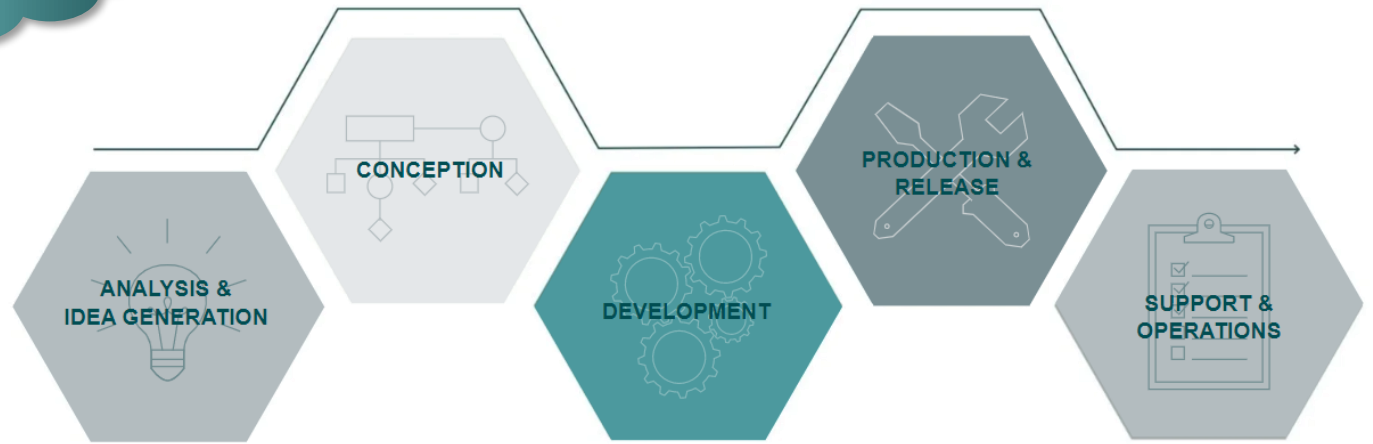
swiss safety center
ISO 9001
ISO 13485
certified system

Mechanical Engineering

Verification & Validation

Startup Support

Software Engineering



Embedded Systems Engineering

Internet of medical things

Material Science

Test Systems

Ziel: Sichere und performante Produkte während gesamtem Lifecycle

See Related Information

Class 2 Device Recall Medtronic MiniMed 600 Series Insulin Pump Systems

Recalled Product

- All MiniMed Remote Controllers (model MMT-500 and MMT-503) used with a Medtronic MiniMed 508 insulin pump or the MiniMed Paradigm family of insulin pumps
- Distribution Dates: August 1999 to July 2018
- Devices Recalled in the U.S.: 31,310
- Date Initiated by Firm: August 7, 2018

Date Initiated by Firm	September 20, 2022
Date Posted	November 08, 2022
Recall Status[1]	Open[3], Classified
Recall Number	Z-0194-2023
Recall Event ID	90910
Product Classification	Pump, infusion, insulin, to be used with invasive glucose sensor - **Product Code** OYC
Product	Insulin Pump/Model: MiniMed 620G/ MMT-1750 MiniMed 640G/ MMT-1711, MMT-1712, MMT-1751, MMT-1752
Code Information	Model/UDI-GTIN (All Serial Numbers): MMT-1750/00763000375461, 00643169559745; MMT-1711/643169554931, 763000367039, 00643169890039, 00643169554917, 00643169629813, 00643169554924, 00643169554931, 00643169742062, 00763000013066, 00643169554948, 00643169554955, 00643169621954; MMT-1712/643169662612, 643169577701, 00763000205409, 00643169890046, 00643169577664, 00643169629820, 00643169577671, 00643169577688, 00763000155346, 00643169577695, 00643169577701, 00643169621961; MMT-1751/643169672239, 00643169574410, 00643169574427, 00643169574434, 00763000253288, 00643169574441, 00643169574458, 00643169643512, 00643169521155, 00643169521704, 00763000015596, 00643169520882, 00643169521421, 00643169521971; MMT-1752/763000192181, 00643169596368, 00643169596382, 00643169596405, 00763000318291, 00763000318307, 00643169596443, 00643169522305, 00643169521292, 00643169522381, 00643169521841, 00643169522268, 00643169521025, 00643169522343, 00643169521575, 00643169522114
Recalling Firm/ Manufacturer	Medtronic MiniMed 18000 Devonshire St Northridge CA 91325-1219
For Additional Information Contact	Medtronic 24-Hr Technical Support 800-646-4633 Ext. 1
Manufacturer Reason for Recall	Medtronic identified a cybersecurity vulnerability in the MiniMed 600 series Insulin Pump Systems associated with the communication protocol that could allow unauthorized access to the pump system. This unauthorized access could be used to deliver too much or too little insulin through delivery of an unintended insulin bolus or because insulin delivery is slowed or stopped, which could lead to hypoglycemia or hyperglycemia. The Remote Bolus feature on insulin pumps should be turned off to prevent the unauthorized access.

HACK

Rückrufaktion für 500.000 unsichere Herzschrittmacher

Rund eine halbe Million Patienten in den USA müssen ins Krankenhaus - und sich ein Firmware-Update für ihren Herzschrittmacher aufspielen lassen. Dieser hatte zuvor Befehle per Funk ohne Authentifizierung akzeptiert.

in Pocket speichern | merken

31. August 2017, 11:30 Uhr, Hauke Gierow

(Bild: St. Jude Medical)

Avast untersucht IoT Devices in Deutschland, Österreich und der Schweiz

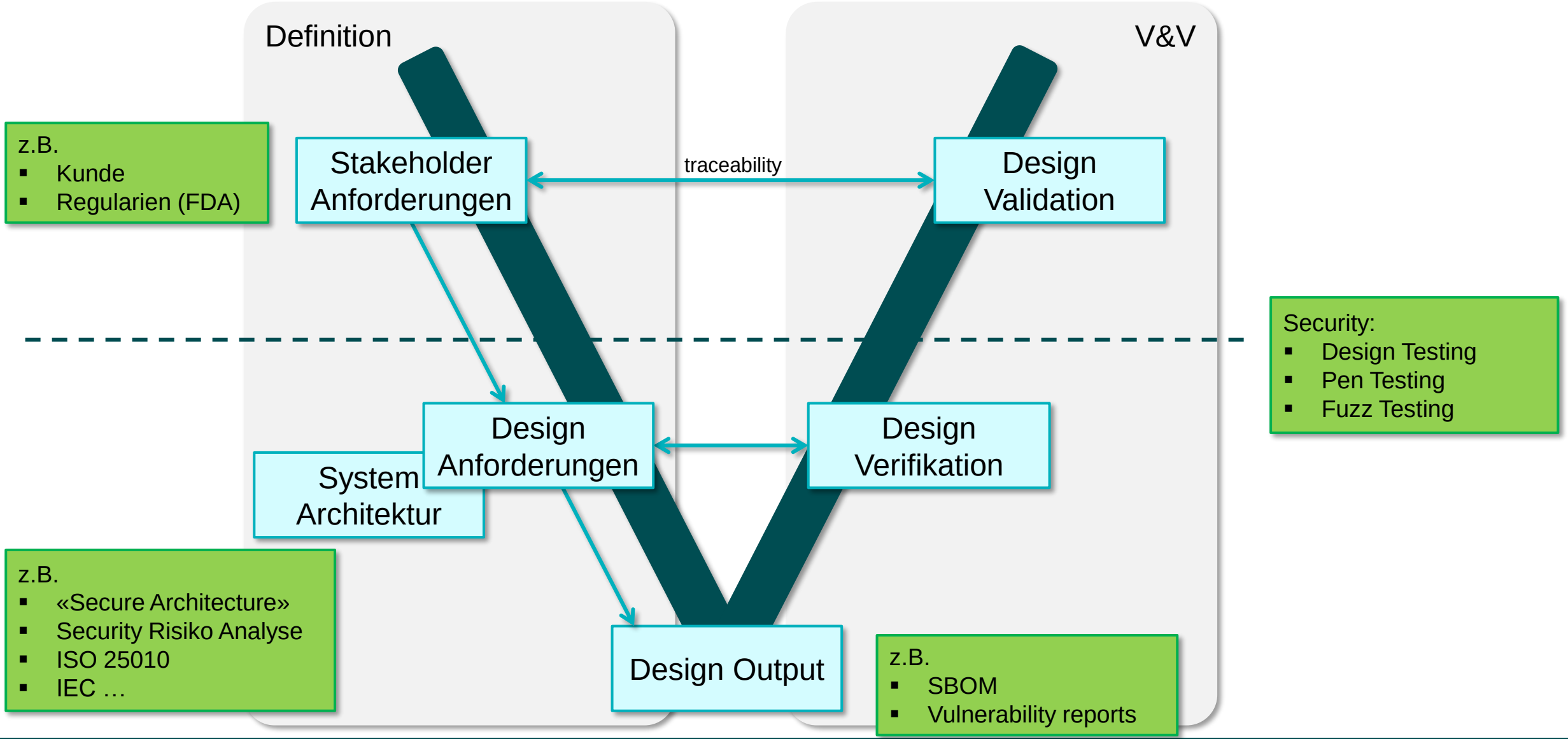
Hunderttausende IoT-Geräte sind unsicher

01.08.2017 Von Jürgen Hill (Chefreporter Future Technologies) FOLGEN

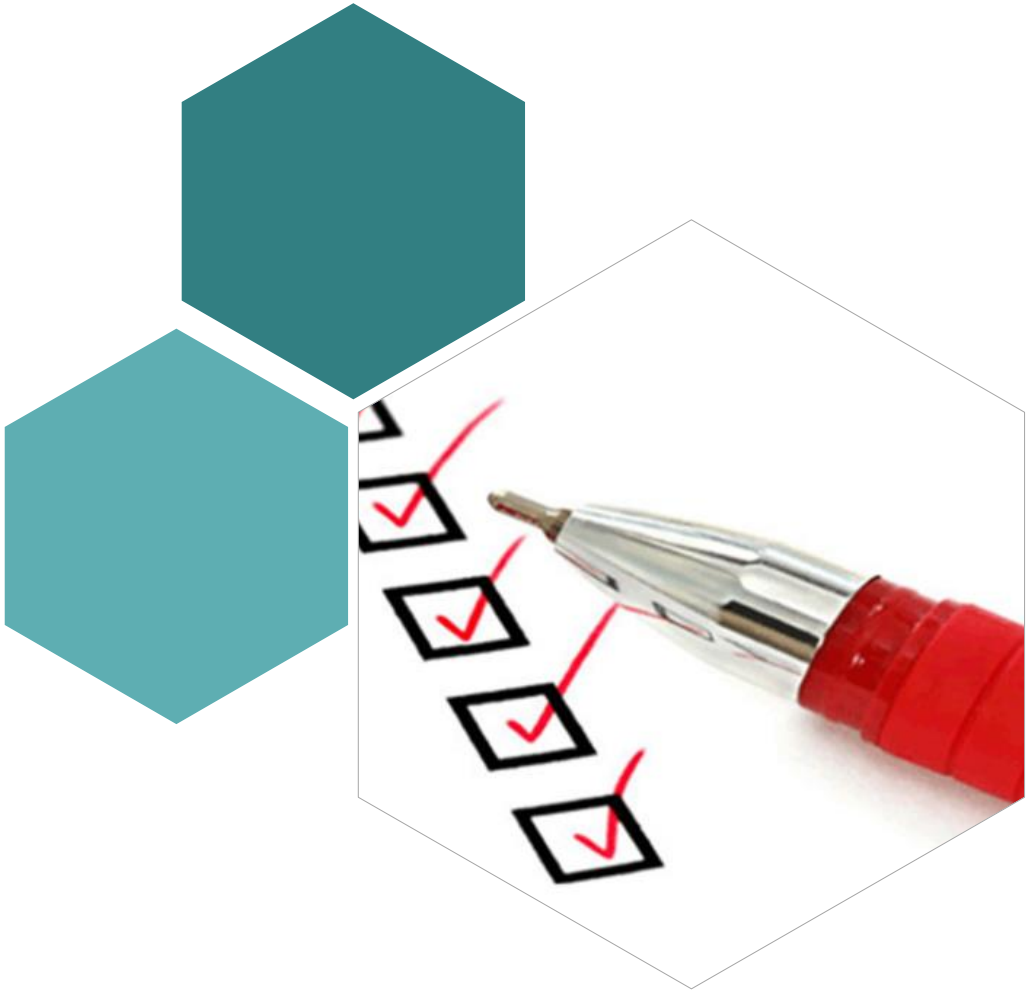
Security-Hersteller Avast hat in DACH die Sicherheit von Smart-Home-Geräten untersucht. Danach weisen hunderttausende IoT Devices Schwachstellen auf und sind eine Einladung für kriminelle Hacker.

Empfehlen
Drucken
PDF
URL
Xing
LinkedIn
Twitter
Facebook
Feedback

Entwicklungsprozess: V - Modell – Security by Design



Herausforderung: Anforderungen



Regularien / Normen

- Übersicht erhalten / behalten
- Richtige Regularien anwenden
- Zurzeit wenig Erfahrung in der (MedTech) Industrie vorhanden

Abwägung

- Benötigte Security-Massnahmen vs. Produkt-Risiken
- Security vs. Ease of Use (Usability)

Unterschiedliche Prioritäten je nach Kunde

- Startups
- KMUs
- Grossfirmen

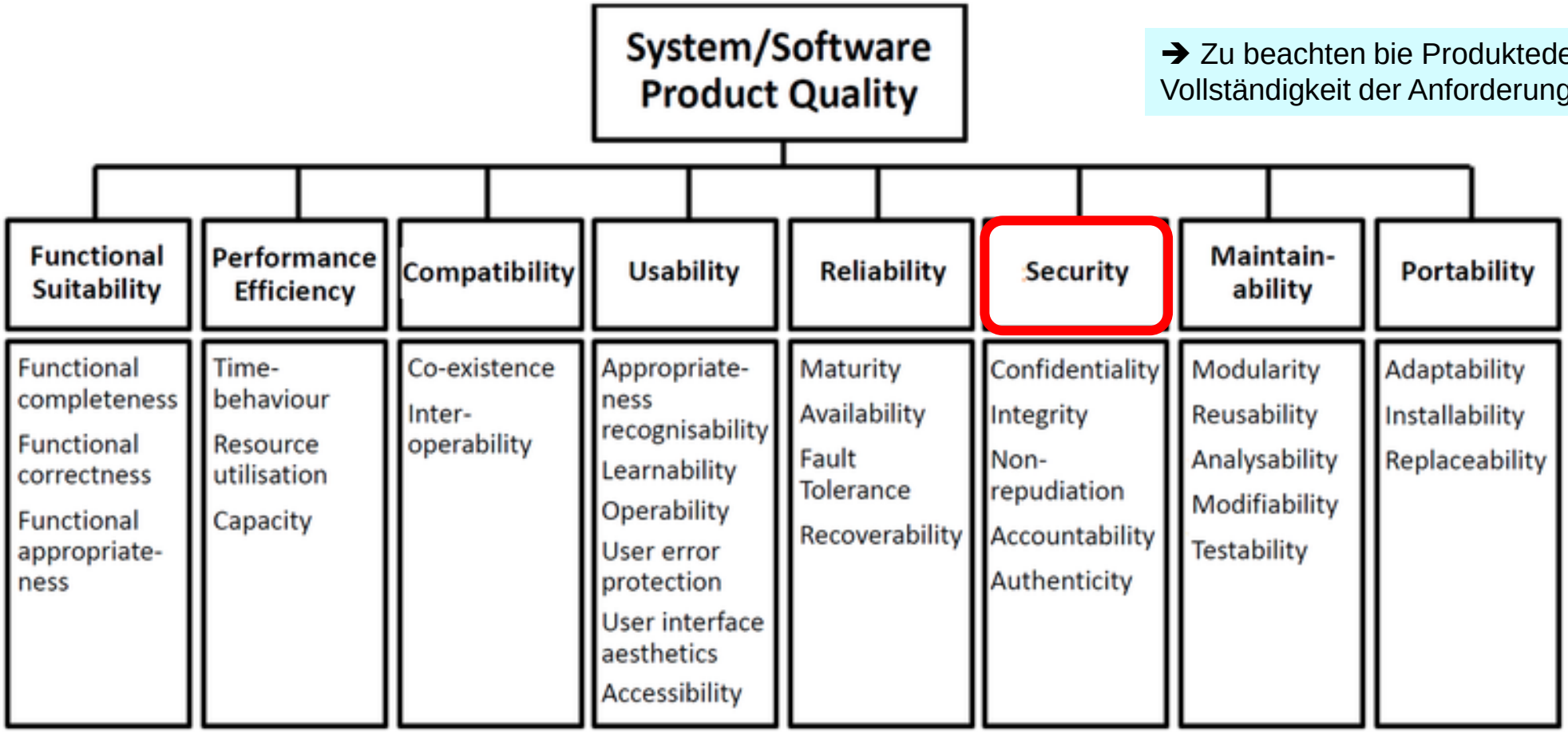
Entwickler

- Benötigte Erfahrung / Affinität zu Cybersecurity

Beispiele Normen / Guidelines (aus MedTech / Industrie)

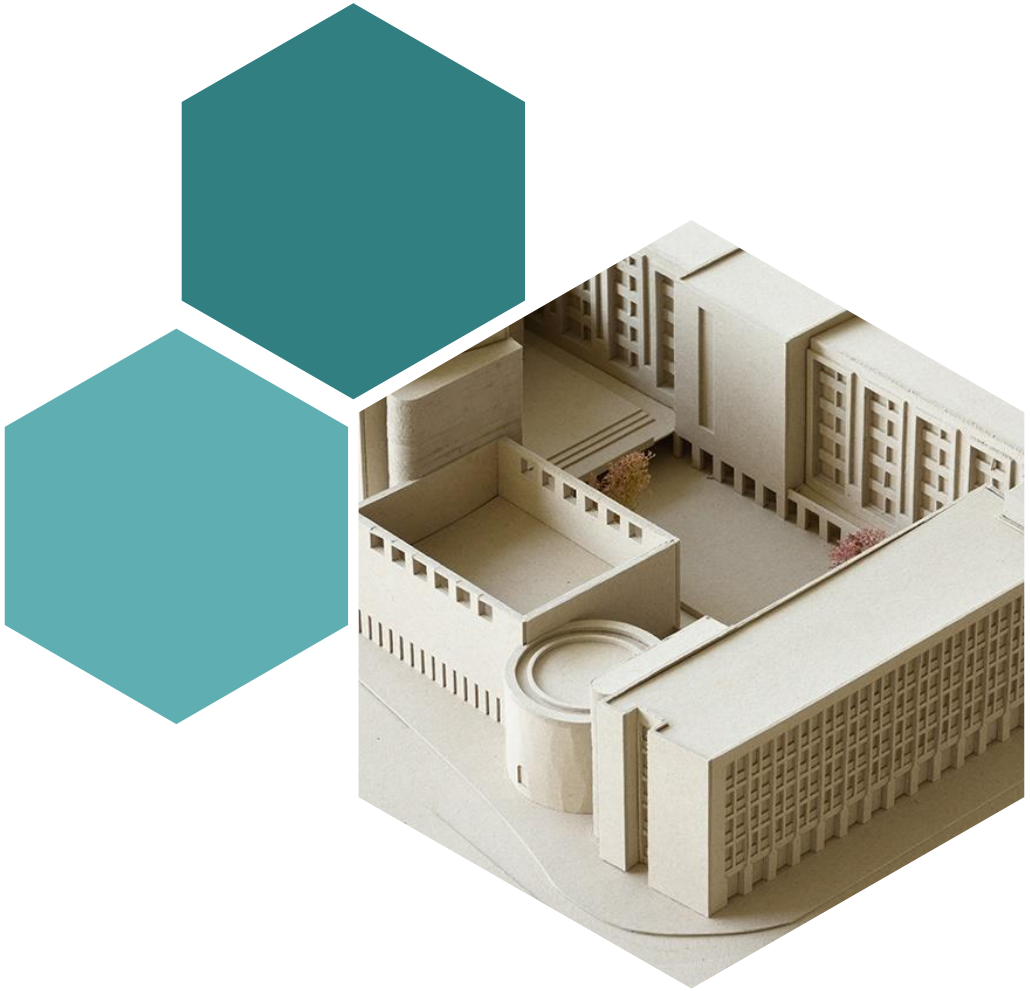
- NIST SP 800-160v1 & v2 Secure Systems, Cybersecurity Framework
- IEC 60601-4-5 Safety-related technical security specifications
- IEC 81001-5-1 Health software and health IT systems safety, effectiveness and security - Part 5-1: Security - Activities in the product life cycle
- IEC 80001-2-x IT-networks
- MDCG 2019-16 Rev.1 Guidance on Cybersecurity for medical devices
- IEC 62443-x-x Security for industrial automation and control systems
- ETSI EN 303 645 / ETSI TS 103 645 Cyber Security for Consumer Internet of Things: Baseline Requirements / ETSI EN ….
- Johner Institut: Leitfaden IT-Sicherheit für Medizinprodukte
- TEAM-NB Position Paper Cyber Security
- AAMI TIR57 Principles for medical device security
- IMDRF Principles and Practices for the Cybersecurity of Legacy Medical Devices, 2022
- IMDRF Principles and Practices for Medical Device Cybersecurity, 2022
- BSI - Standards and Certification (bund.de) / Cyber-Sicherheitsbetrachtung vernetzter Medizinprodukte (BSI Projekt 392 ManiMed)
- FDA Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions - Draft Guidance, 2022
- …

ISO 25010 – Qualitäts-Anforderungen (Nichtfunktionale Anforderungen)



➔ Zu beachten bie Produktedesgin ➔ Überprüfung der Vollständigkeit der Anforderungen

Herausforderung: System-Architektur



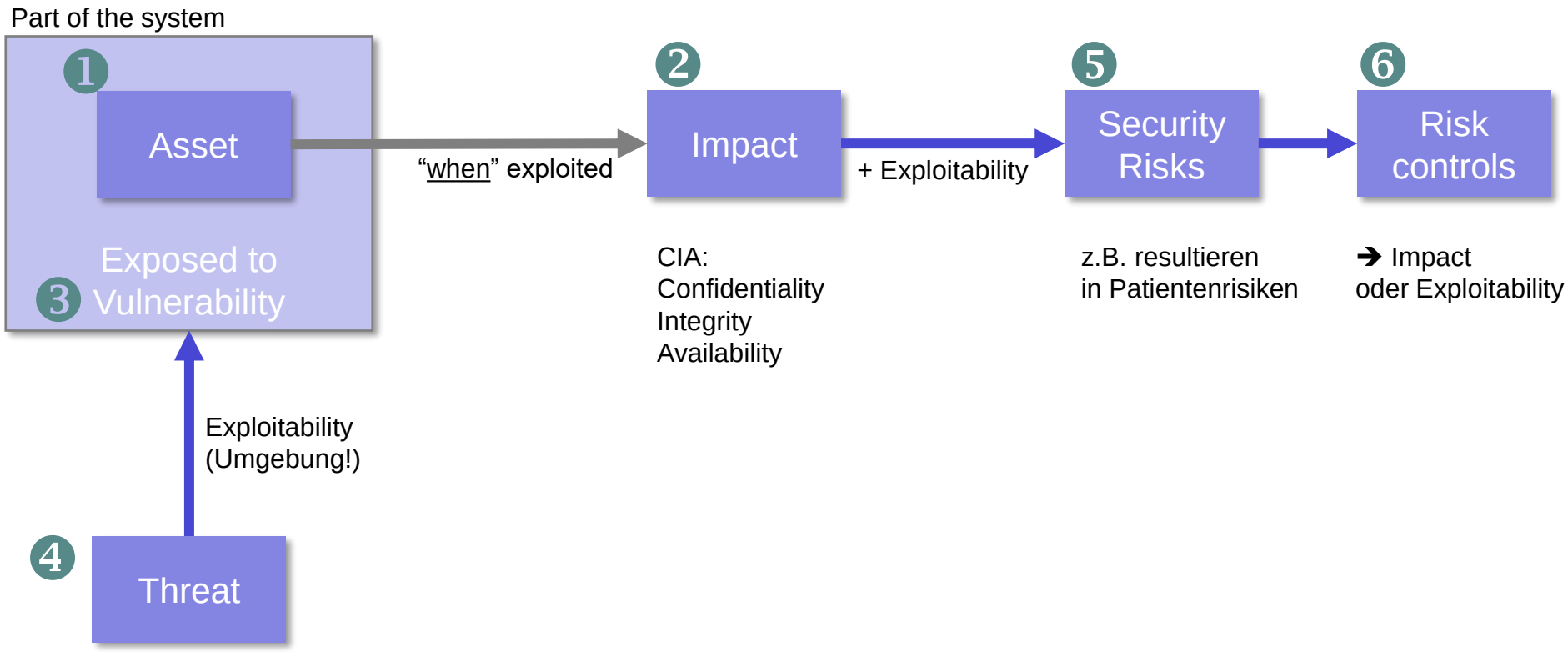
- **Shared Responsibility**
- **Technologie-Entscheide**
- **Design-Entscheide**
- **Third-Party Komponenten**
- **Bewusstsein / Security by Design / Lifecycle**
- **Bewährte Methodiken / Best-Practice Algorithmen einsetzen**
- **Organisation und Struktur beeinflussen System-Architektur!**

Security Risiko Analyse - Wichtiger Input zur System-Architektur

z.B.
Patientendaten
Konfigurationsparameter
Firmware Image

z.B.
USB
Bekannt Bugs
Fehlende Authentisierung
…

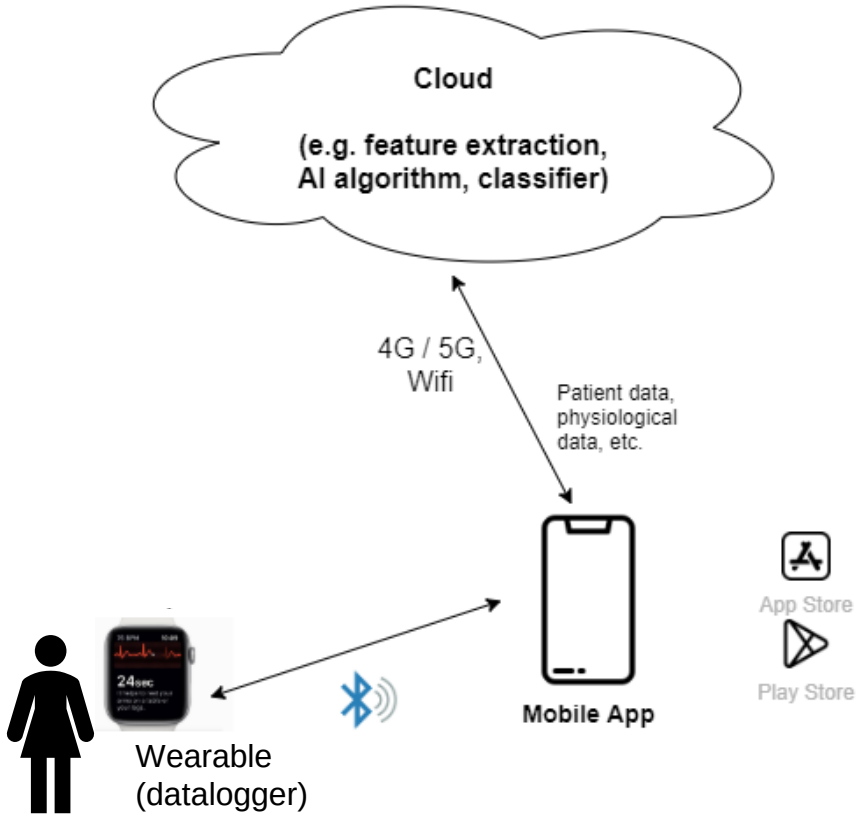
z.B. STRIDE Methode für
Threat Modeling



Design Output

- **Built Pipeline**
- **Software BOM**
- **Vulnerability scans (3rd party)**
- **Minimum Features:**
  - Authentisierung
  - Verschlüsselung

Beispiel: Fruchtbarkeits-Tracker



Zweckbestimmung:
- Fruchtbare Tage bestimmen

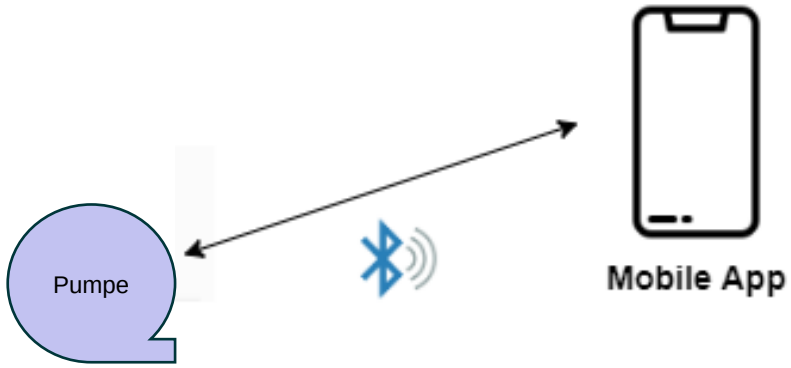
Architektur
- Keine Patientendaten auf dem Wearable
- Mobile App als Gateway und für Daten-Visualisierung
- Login-Daten und physiologische Daten getrennt in Cloud
- Keine Authentisierung bei BLE benötigt
- Proprietäres Protokoll bei BLE, keine Verschlüsselung

CIA-Impact: Integrity!
- Threat: Man-in-the-middle

Security-Risiko: eher hoch
Patienten-Risiko: niedrig / keine

Marktzulassung 2020 (FDA)

Beispiel: Insulin-Pumpe



Zweckbestimmung:
- Autonome Insulinabgabe

Architektur
- Mobile App zur Konfiguration und für Daten-Visualisierung
- Minimale Patientendaten auf dem Wearable
- Keine Patientendaten auf Mobile Phone
- Authentisierung: User Interaktion benötigt
- Proprietäres Protokoll mit Verschlüsselung
- Kommunikation nur während User-Interaktion möglich
- Keine Internetverbindung

CIA-Impact: Integrity!
- Threat: Man-in-the-middle

Security-Risiko: niedrig
Patienten-Risiko: hoch

Noch nicht auf dem Markt

Take Home Messages

- **«Stand der Technik» bei Entwicklungsstart beachten**
- **CIA Analyse und Threat-Modeling früh in der Entwicklung starten**
- **Produkt-Lebenszyklus und Marktüberwachung in der Entwicklung beachten**
- **Beurteilen und begründen, was “genug” Sicherheit für das jeweilige Produkt ist**

Vielen Dank!

Ivo Locher, PhD, EMBA, PMP
Program Manager at konplan

https://www.linkedin.com/in/ilocher/

+41 41 799 30 10

ivo.locher@konplan.com

konplan

konplan ag
Suurstoffi 2
CH-6343 Rotkreuz