Spital Thurgau

thurmed

Interoperabilität mit hoher Sicherheit erreichen wir nur gemeinsam!

Aus Sicht ICT Infrastruktur
und klinischer Applikation

thurmed

Spital Thurgau

Venenklinik Bellevue
Ihre Spezialklinik am Bodensee

RVZ Rheumatologisches Versorgungszentrum Weinfelden

Praxisgemeinschaft Storchen Stein am Rhein

milagro
Kinderwunsch- und IVF-Zentrum

Team Radiologie PLUS

RABAG Radiologie am Bahnhof in Frauenfeld[2]
RIWAG Radiologisches Institut in Weinfelden
RNO Radiologie Nordost in Goldach
RNO Radiologie Nordost in Heerbrugg
RNO Radiologie Nordost in Romanshorn
RNO Radiologie Nordost in St. Gallen
RNO Radiologie Nordost in Wattwil
RSO Radiologie Südost in Chur am Bahnhof
RSO Radiologie Südost in Chur Belmont
RSO Radiologie Südost in Bad Ragaz[1]
RSO Radiologie Südost in Buchs[1]

Spitalpharmazie Thurgau

thurmed IMMOBILIEN

Spitalcampus Apotheken Thurgau

WÄSCHEREI BODENSEE AG
Textil-Logistik & Mietwäsche
WÄSCHEREI MITTELLAND

Horizont Apotheke[1]

wäscherei regio

Spital Thurgau

Christoph Knöpfel

Ausbildung

- EL. Ing HTL/FH (1994-1997)
- Master Medical Informatics (seit 2008)
- IPMA B Zertifizierung(seit 2018)

Arbeiten

- Medizintechnikbranche ca. 10 Jahre
- Medizininformatik seit 15 Jahren
- IHE International seit 1999
- Seit 1 Jahr beim Spital Thurgau
  Abteilungsleiter klinische Applikationen

Spital Thurgau

Roger Nobel

Ausbildung

- EL. Ing HTL/FH (1994-1998)
- Aktiv CCIE# 23679 Enterprise (seit 2009)
- eMBA Business Innovation (2014-2016)

Arbeiten

- Software Entwickler bei Siemens
- Über 20 Jahre bei Cisco System
  Technical Leader im Technical Service (TAC)
- Seit 2 Jahren beim Spital Thurgau
  Abteilungsleiter ICT Infrastruktur

Spital Thurgau

Agenda

- Ausgangslage
- Netzwerksegmentierung
- Zonen Microsegmentierung
- Intend Based Networking
- Endpoint Security
- Security Operation Center
- Fernzugänge
- SDC als neuen Standard bei MT Geräten

Spital Thurgau

Ausgangslage

Alle sprechen von Interoperabilität. Dennoch kämpfen wir mit «einfachen» Problemen.

- Welcher Virusschutz verträgt sich mit allen Applikationen?
- Welche SW/HW kommuniziert wirklich im Netzwerk?
- Wie kann ich Risiken überwachen ohne immer gleich einen kompletten Ausfall zu riskieren?
- Wieso kennt der eine Lieferant nur A und der andere nur B?

Spital Thurgau

Netzwerksegmentierung

Insgesamt trägt die Netzwerksegmentierung wesentlich zur **Verbesserung der Sicherheitsarchitektur** eines Netzwerks bei und ermöglicht eine gezielte Verwaltung und Optimierung des Netzwerkverkehrs.

Zonierung für North-South Traffic im Campus und RZ

- Isolierung von sensiblen Daten und kritischen Bereichen
- Spezifische Zugriffsrechte und Sicherheitsrichtlinien für verschiedene Netzwerksegmente.
- Kontrolle über den Datenverkehr und Verbesserung der Sichtbarkeit.
- Schadensbegrenzung bei Malware und anderen schädlichen Aktivitäten.
- Einfache Fehlerbehebung bei Problemen oder Sicherheitsvorfällen

Spital Thurgau

Zonen Microsegmentierung

Während herkömmliche Netzwerksegmentierung das Netzwerk in grössere Segmente unterteilt, geht die Microsegmentierung auf eine viel granularere Ebene, indem sie einzelne virtuelle Maschinen (VMs), Container oder sogar spezifische Anwendungskomponenten segmentiert.

- Segmentierung von East-West Traffic innerhalb der RZ Zonen
- Zero-Trust-Architektur im Campus
  Durch die Anwendung einer Zero-Trust-Architektur kann jeder Kommunikationsversuch innerhalb des Netzwerks überprüft und authentifiziert werden, unabhängig davon, ob er innerhalb oder ausserhalb des Netzwerkperimeters stattfindet.

Spital Thurgau

IntenT Based Networking

Intent-Based Networking (IBN) zielt darauf ab, die **Netzwerkkonfiguration und -verwaltung zu automatisieren und zu vereinfachen**, indem sie die Absichten (Intents) des Netzwerkadministrators in konkrete Netzwerkpolicies und -aktionen umsetzt.

- Network Access Control mit dynamischer Netzwerksegment Zuweisung.
  - Authentication wer sich am Netzwerk verbinden will
    - Zentrale Verwaltung von Geräten und Benutzer
  - Authorization Erlaubnis wo man sich verbinden darf. Somit eine automatische Zuweisung in ein Netzwerksegment (VLAN).
  - Accounting zu Aufzeichnung
- Wenig Bedarf an manueller Netzwerk Konfiguration im Access. Man kann alle Geräte überall anschliessen und das Netzwerk konfiguriert sich selbst und reduziert so menschliche Fehler, verbessert die Sicherheit und Leistung des Netzwerks.

Spital Thurgau

Endpoint Security

- **Endpoint Security mit XDR "Extended Detection and Response"**
  - XDR integriert verschiedene Sicherheitslösungen wie Endpoint Detection and Response (EDR), Network Traffic Analysis (NTA), Security Information und Event Management (SIEM), Cloud Security und mehr. Diese Integration ermöglicht eine umfassendere Sicht auf Sicherheitsereignisse und Bedrohungen.
  - XDR verwendet fortschrittliche Analysen und maschinelles Lernen, um Bedrohungen zu erkennen, die traditionelle Sicherheitslösungen möglicherweise übersehen.
  - XDR-Lösungen bieten automatisierte Reaktionsmechanismen, die schnell und präzise auf erkannte Bedrohungen reagieren können. Dies reduziert die Zeit, die erforderlich ist, um auf Vorfälle zu reagieren, und minimiert potenzielle Schäden.
  - XDR ist darauf ausgelegt, sich an neue und sich weiterentwickelnde Bedrohungen anzupassen. Durch kontinuierliche Überwachung und Updates bleibt die Sicherheitslage eines Unternehmens robust und widerstandsfähig gegenüber neuen Angriffstechniken.
- **Zertifikatbasierende Ausnahmen**
  - Durch das Signieren der Software mit digitalen Zertifikaten stellen wir sicher, dass Nutzer und Systeme die Authentizität und Integrität der Software verifizieren können. Dies schützt sowohl den Hersteller als auch die Endnutzer vor Manipulationen und Missbrauch. Das sollte eigentlich in der Medizin Software ein Standard sein.
  - Die MDR (Medical Device Regulation) ebenso ISO 13485 schreibt vor, dass Hersteller von Medizinprodukten (inkl. Software) Massnahmen ergreifen müssen, um die Integrität und Sicherheit ihrer Produkte zu gewährleisten. Dies umfasst auch den Schutz vor unbefugtem Zugriff und Manipulation.

Spital Thurgau

Security Operation Center

- SOC überwachen kontinuierlich Netzwerke, Systeme und Datenverkehr, um proaktive Bedrohungserkennung und verdächtige Aktivitäten oder Anomalien zu erkennen 24/7/365.
- Bei einem Sicherheitsvorfall reagieren SOC-Teams schnell, um den Vorfall zu untersuchen, zu isolieren und zu beheben.
- Ein SOC kann langfristig Kosten sparen, indem es teure Sicherheitsvorfälle verhindert und die Effizienz der Sicherheitsoperationen erhöht.

Spital Thurgau

Fernzugänge und Maintenance

Ein Fernzugang ermöglicht es Benutzern, auf ein Netzwerk, Systeme oder Daten eines Unternehmens von einem entfernten Standort aus zuzugreifen. Dies ist besonders wichtig für mobile Arbeitskräfte, Telearbeit und externe Dienstleister, die von ausserhalb des Unternehmensnetzwerks auf wichtige Ressourcen zugreifen müssen. Der Fernzugang kann über verschiedene Technologien realisiert werden.

- **Fernzugang für Monitoring**
  - S2S VPN, für eine permanente Verbindung
  - Firewall sollte nur Traffic fürs Monitoring erlauben
- **Maintenance**
  - Zwei-Faktor-Authentication (2FA)
  - Remote Zugriff Tool mit Aufzeichnungsmöglichkeit.
  - Jump Host, um auf weitere Systeme zu gelangen
- **Update von Repository Server des Hersteller.**
  - SFTP / SCP, um gezielt Files zu kopieren
  - Kopie Start über die Maintenance Verbindung initiieren

Spital Thurgau

IEEE 11073 Service-oriented Device Connectivity (SDC)

SDC wird hauptsächlich von OR.NET e.V. vorangetrieben

Im OR.NET e.V. haben sich Akteure aus Industrie, Klinik und Forschung zusammengeschlossen, um gemeinsam den **offen vernetzten OP-Saal der Zukunft** zu realisieren.

Inhalte und Bilder stammen von ornet.org

Spital Thurgau

IEEE 11073 Service-oriented Device Connectivity (SDC)

Die wichtigste Funktionen, welche durch die Nutzung des SDC-Protokolls ermöglicht werden sind:

- **Bidirektionaler** Datentransfer zwischen einer Vielzahl von Medizingeräten unterschiedlicher Hersteller
- **Fernsteuerung** einzelner Funktionen
- Konsistente Daten und hohe Datenqualität durch **standardisierte Kommunikation**

Inhalte und Bilder stammen von ornet.org

Spital Thurgau

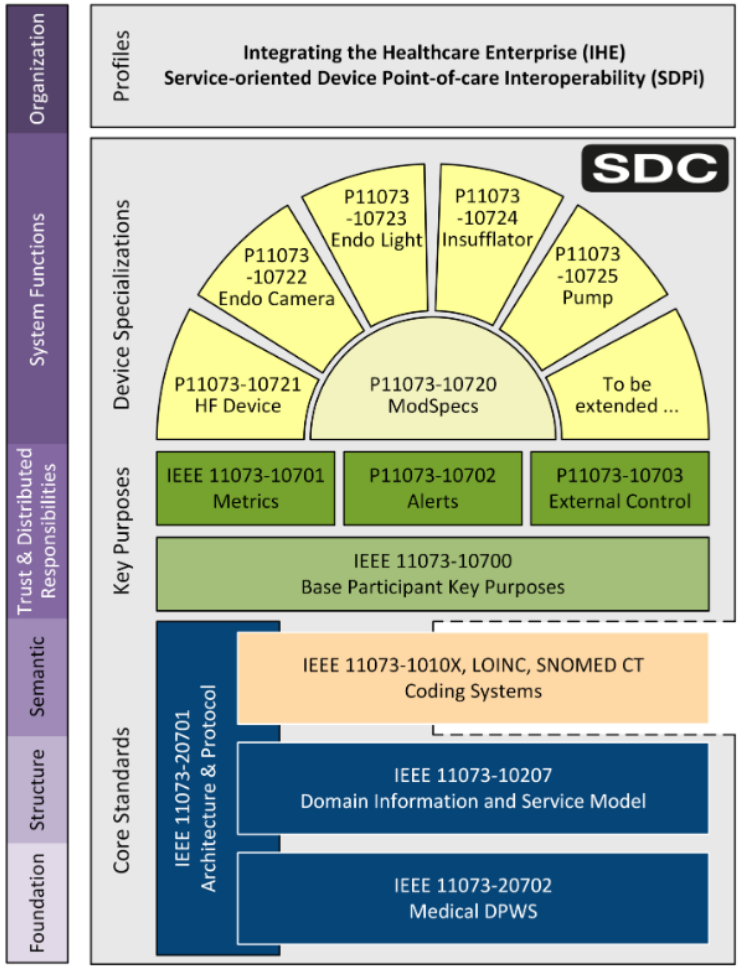
IEEE 11073 Service-oriented Device Connectivity (SDC)

Die Kernnormen definieren den **Transportmechanismus** (ISO/IEEE 11073-20702) und das **Domain Informations- und Servicemodell** (ISO/IEEE 11073-10207).

Die dritte Norm, ISO/IEEE 11073-20701, beschreibt die **Architektur und die Verbindung** der beiden zuvor genannten Normen.

Die IEEE 11073-1010X beschreibt die **notwendige Semantik**, die aber auch durch LOINC oder Snomed-CT **ergänzt** werden kann.

Die PKP-Standards (siehe grüner Teil der Abbildung) definieren **technische, prozessuale und dokumentarische Anforderungen**, um eine **sichere** und effektive Verbindung zwischen medizinischen Geräten verschiedener Hersteller zu gewährleisten.



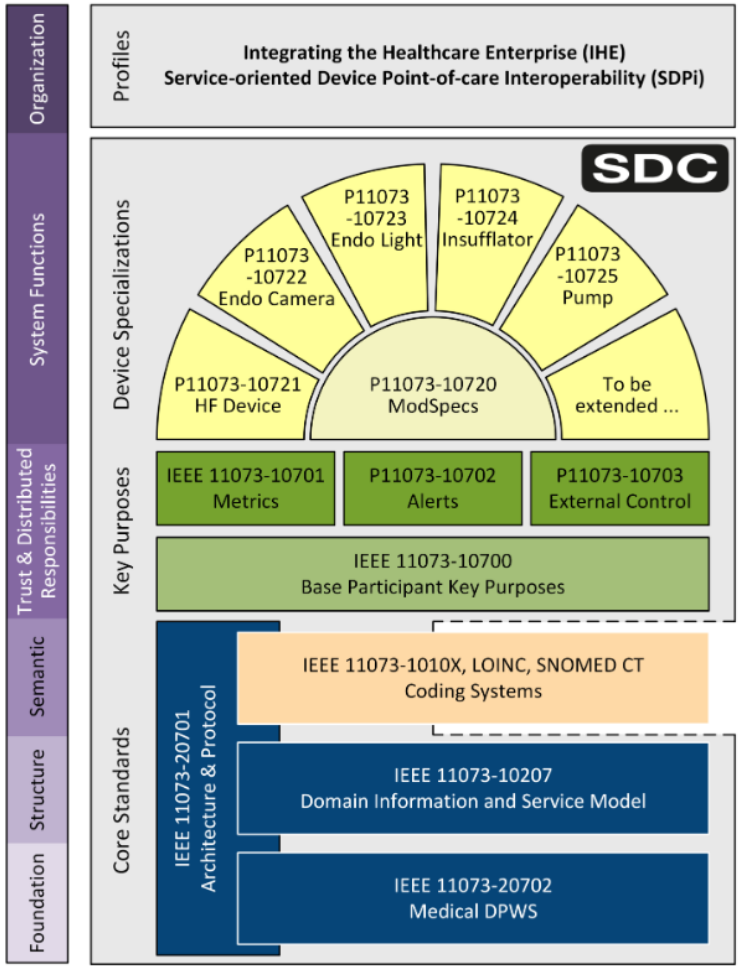
Inhalte und Bilder stammen von ornet.org

Spital Thurgau

IEEE 11073 Service-oriented Device Connectivity (SDC)

Während Core Standards (blau) und PKP (grün) allgemein gehalten sind, sind die DevSpecs spezifisch für eine **bestimmte Klasse** von Medizinprodukten.

Die SDC-Normenfamilie wird durch das **IHE-Profil SDPi (Service-oriented Device Point-of-care Interoperability)** ergänzt. Im Sinne der IHE werden Anwendungsfälle definiert und die Standards verfeinert.



Inhalte und Bilder stammen von ornet.org

„SDC Cathedral Window (Version 2.1)", Martin Kasparick and Björn Andersen, Licence:

Spital Thurgau

IEEE 11073 Service-oriented Device Connectivity (SDC)

Ganz nach dem Spirit der IHE Initiative bringt SDC allen einen **Nutzen auch bezüglich Sicherheit**

- Dank der **zertifikatsbasierten Kommunikation** kann die Endpoint Security verbessert werden
- Dank der Beschreibung der Dokumentationspflicht ist ein **Risikomanagement gemäss EN 80001-1** (Risikomanagement von MT-Produkten in Netzwerken) mit weniger Missverständnissen umzusetzen

Inhalte und Bilder stammen von ornet.org

Spital Thurgau

DANKE!

Christoph Knöpfel Abteilungsleiter klinische Applikationen
christoph.knoepfel@stgag.ch

Roger Nobel Abteilungsleiter ICT Infrastruktur
roger.nobel@stgag.ch