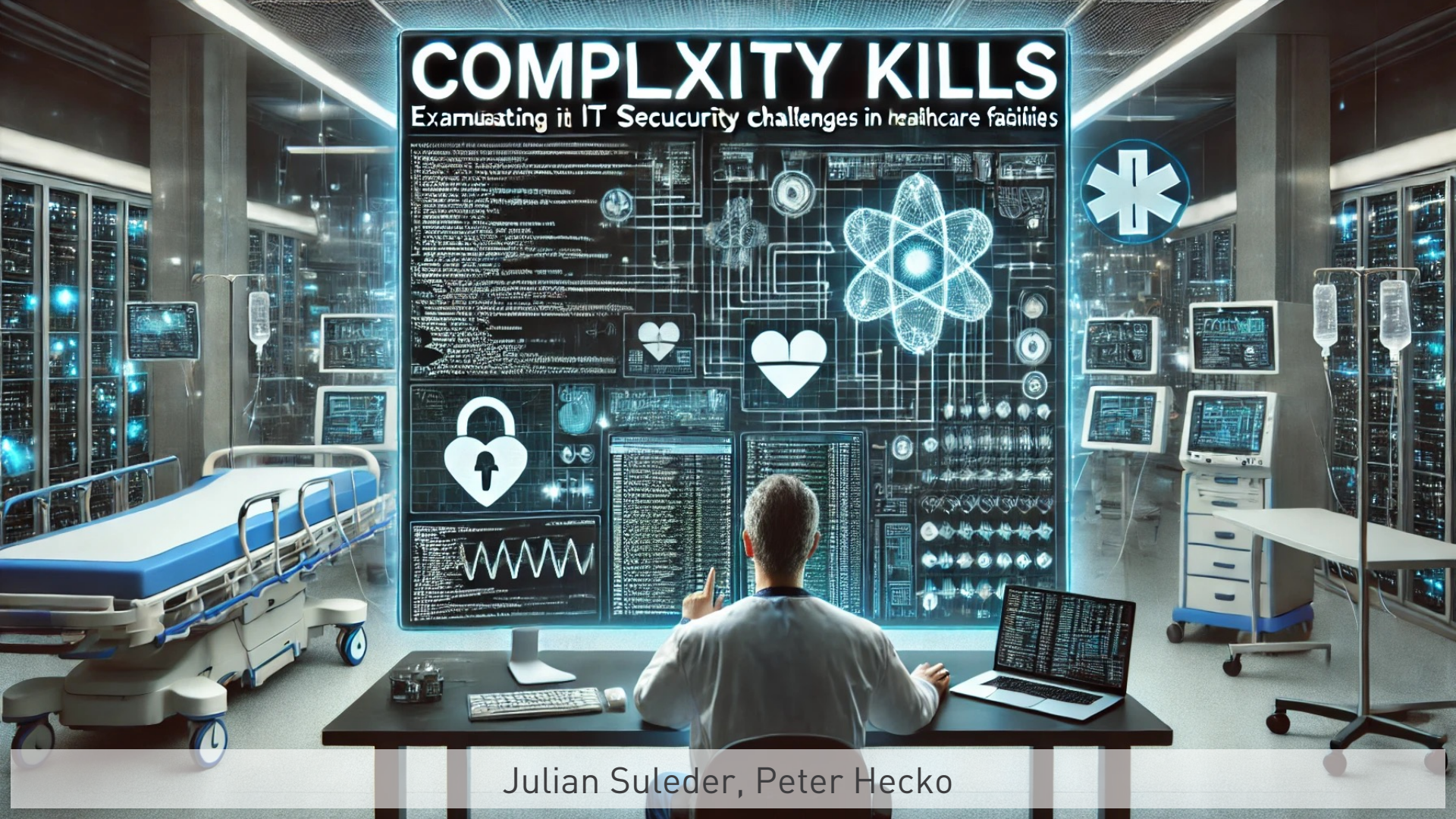


Julian Suleder, Peter Hecko

ERNW
providing security.

Who We Are

- Julian Suleder
  - Senior Security Analyst & Researcher @ ERNW
  - Medical computer science background
  - Performing medical device security assessments
- Peter Hecko
  - Head of the Cyber Defense Center at HELIOS Kliniken
  - Podcaster
  - Long-standing member of the Chaos Computer Club (CCC)

ERNW
providing security.

Quantifying Helios Kliniken GmbH

- ~89 hospitals , ~230 medical care centers (MVZ)
- ~5.5m people treated, >4m on an outpatient basis
- ~78,000 employees in Germany, 7.3b € revenue (2023)
- >62.000 clients, >10.000 server hosts
- Active Directory: >140.000 users, >130.000 groups, >150 DCs
- >35.000 medical devices (IoMT), ~60% networked
- SOC: >40 incidents / day, 18 employees

ERNW
providing security.

Regulatory Requirements

- Regulation (EU) 2017/745 - Medical Device Regulation (MDR)
- §8 BSIG & BSI-Kritisverordnung - BSI-KritisV
- BSI TR-03161: Anforderungen an Anwendungen im Gesundheitswesen
- DKG: Branchenspezifischer Sicherheitsstandard (B3S): Informationssicherheit im Krankenhaus
- Krankenhauszukunftsgesetz* (KHZG)

* min. 15% “Maßnahmen zur Verbesserung der Informationssicherheit“

Regulatory Requirements

Challenges

ERNW
providing security.

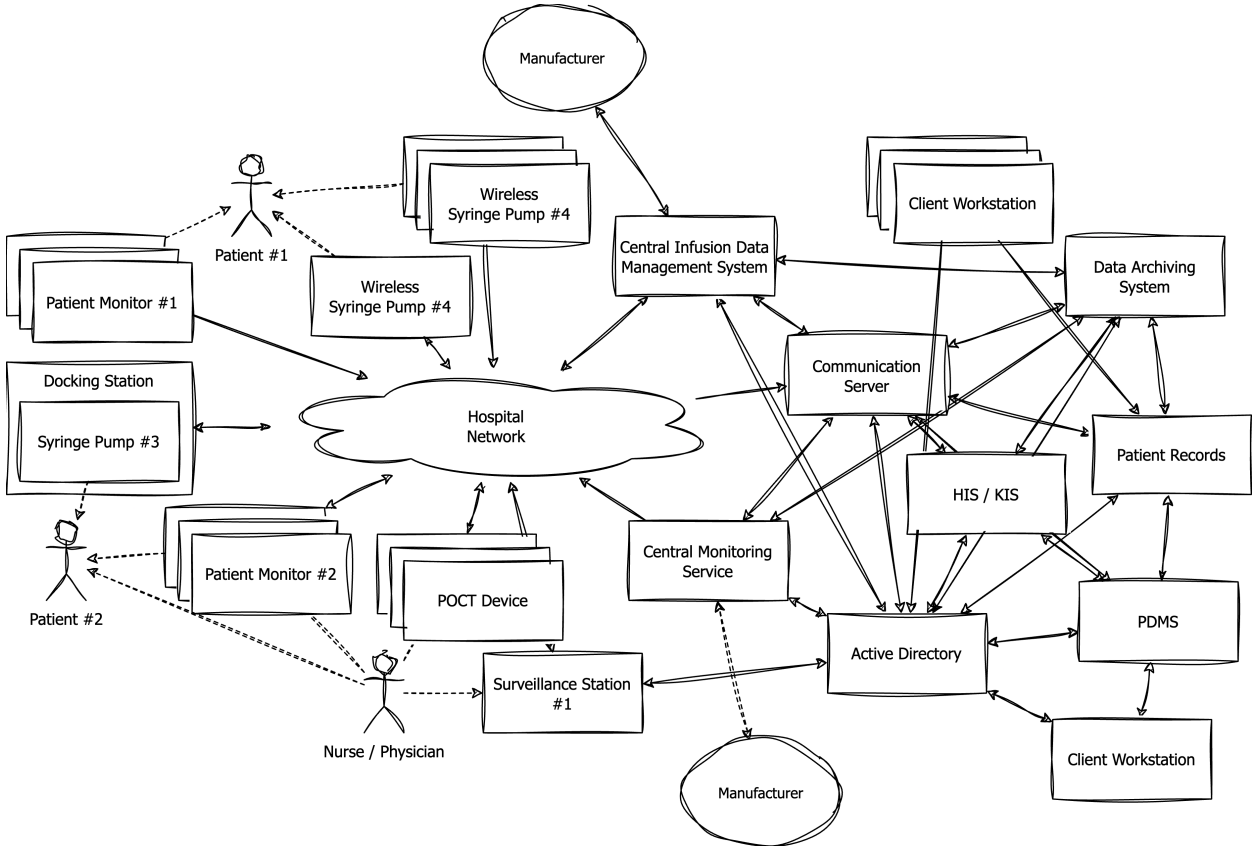
Challenge: Publicly accessible buildings

- Many publicly accessible and shared areas
- No closing times – 24/7 operation
- Huge buildings and areas that are difficult to survey and monitor
  - Presence of IT, OT and medical devices (IoMT) almost everywhere
  - Thousands of network ports with different networks
  - Access controls difficult to implement at network level
  - Many areas where infrastructure is unobserved
  - Flexibility is absolutely essential
- Use of electronic door locking systems where possible

Challenge: Medical Device Systems

- Often: Manufacturer's software stack on hospital-supplied host
  - → Operation of grey or black boxes within the core infrastructure
- Communication of the IoMT ecosystem with third-party systems
  - Various update processes / remote management solutions
  - Requirements for user and authorization management → AD integration
  - Compatibility assurance: secure and insecure protocols available at once
- Integration into backup processes
- → IT security risks hardly observable
- → Joint effort with manufacturers ☺

Our Exemplary Hospital...



Not enough Complexity?

Supporting Processes

- Central hospital pharmacy, laboratory & radiology
- Patient administration and billing
- Facility & building services

Communication

- Pager and nurse call systems
- Telephony & entertainment systems
- Medical communication server
- Telemedicine applications

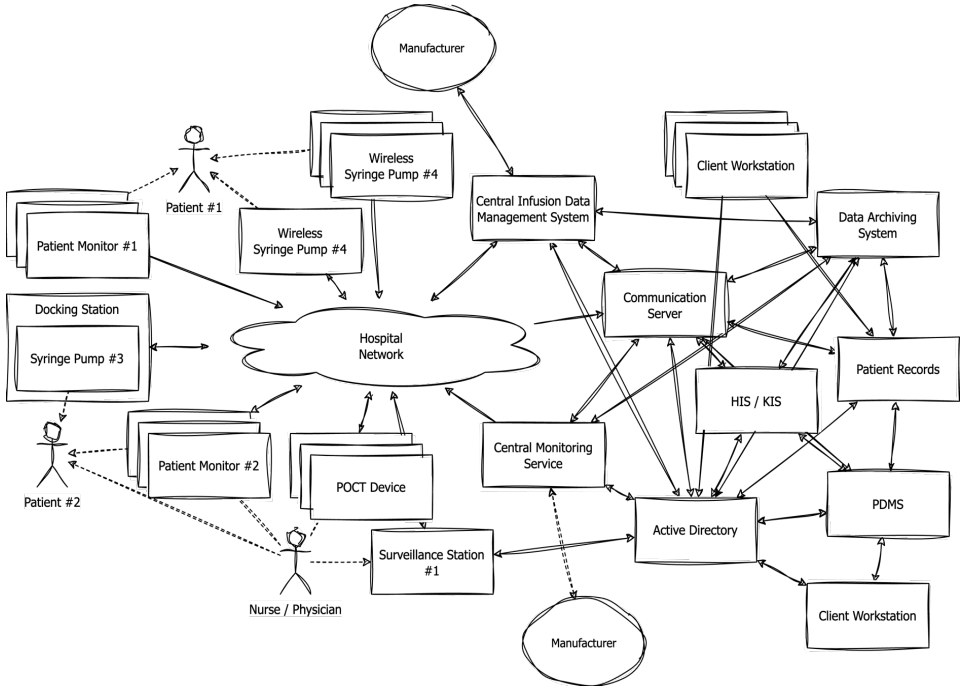
Administrative Processes

- Quality and risk management
- Resource Management
  - Surgery planning & appointment scheduling
  - Laundry & cleaning, sterile processing
  - Purchasing processes & controlling

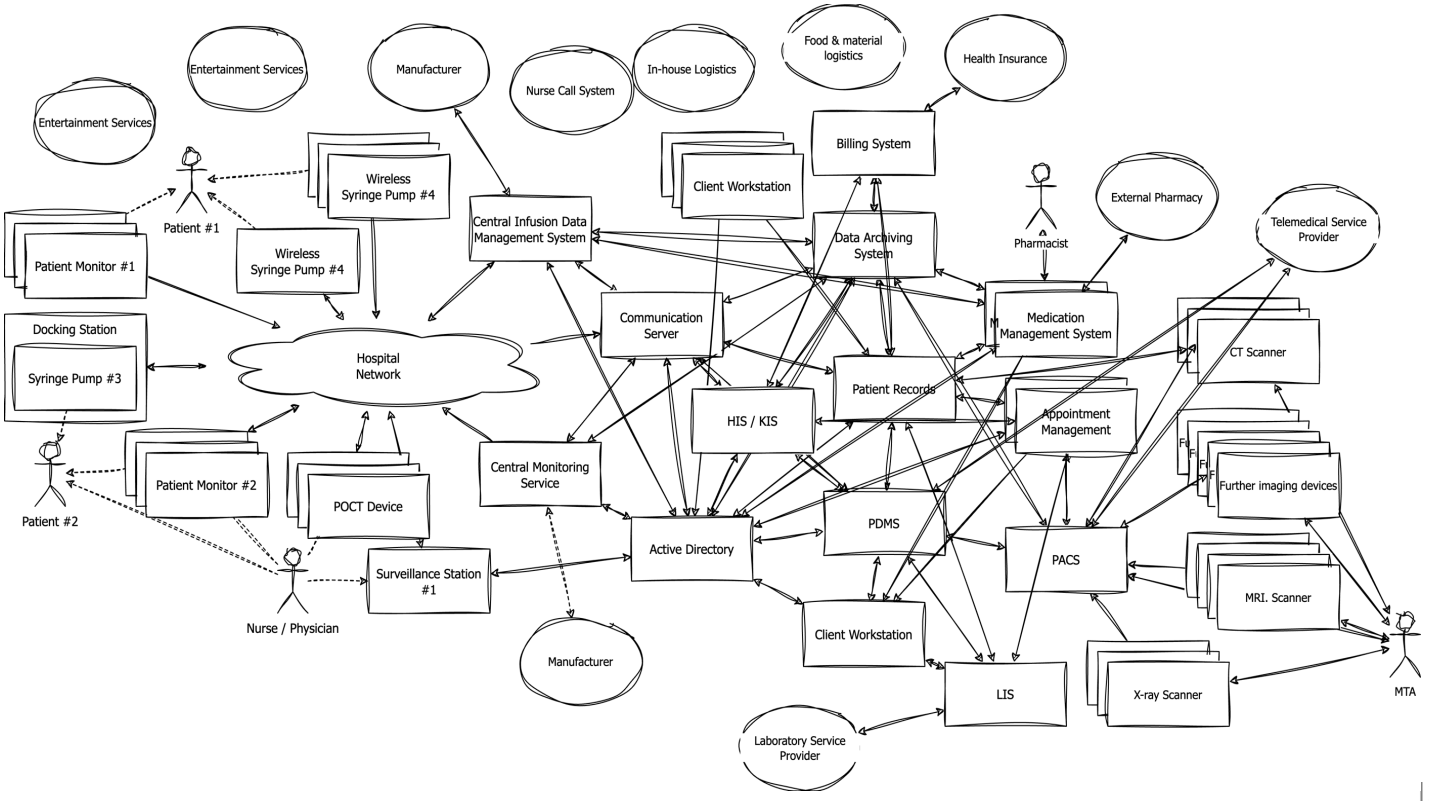
In-house logistics

- Supply of technical gases
- Food & material logistics
- Medication supply
- In-house mail, pneumatic tube, specimen & patient transfer, ...

Our Exemplary Hospital ...



Our Exemplary Hospital …



ERNW
providing security.

Challenge: Human Resources

- Structural and sector-related tight financial situation
- Compensation and revenue very difficult to scale
- Huge recruitment problems in every profession / high vacancy
- Competition with industries with "*less complex*" problems, but more resources
- Historical subordination of IT to medical or administrative management / conflicts with “principalities”
- Pandemic increased all these problems!

Approach: IT & Operational Centralization

- Implementation of a central ITSM, SOC
- Centralization of core infrastructure and medical systems
  - Internal and external hosting
  - Remote access
  - Backup and failure / recovery processes
  - Identity & access management
- → Share resources between different locations!
  - Security monitoring and support processes
  - Service orientation, standardization and harmonization

ERNW
providing security.

Sounds great, but..

- Good approach if you have enough resources!
- You have to change your infrastructure during 24/7 operation
- Barely feasible with the IT department of one hospital
- You will never have a „clean“ environment as a starting condition

“Clean” Environments

- There is just a certain level of „clean“
- Establishing standard core infrastructure, standards and procedure is much easier
- Still dealing with the same IoT and IoMT vendors and products

ERNW
providing security.

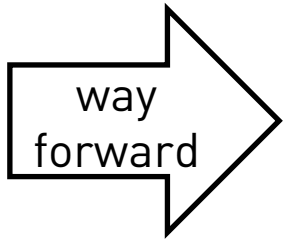
How to deal with legacy environments?

- → Know your weak spots & monitor them!
  - Perform a risk analysis of your assets
- Step-by-step replacement of existing systems
- Analysis of to be newly introduced systems for security capabilities through e.g. external penetration tests
- Development of security concepts including emergency and recovery plans together with the manufacturer/vendor

tough

cookie

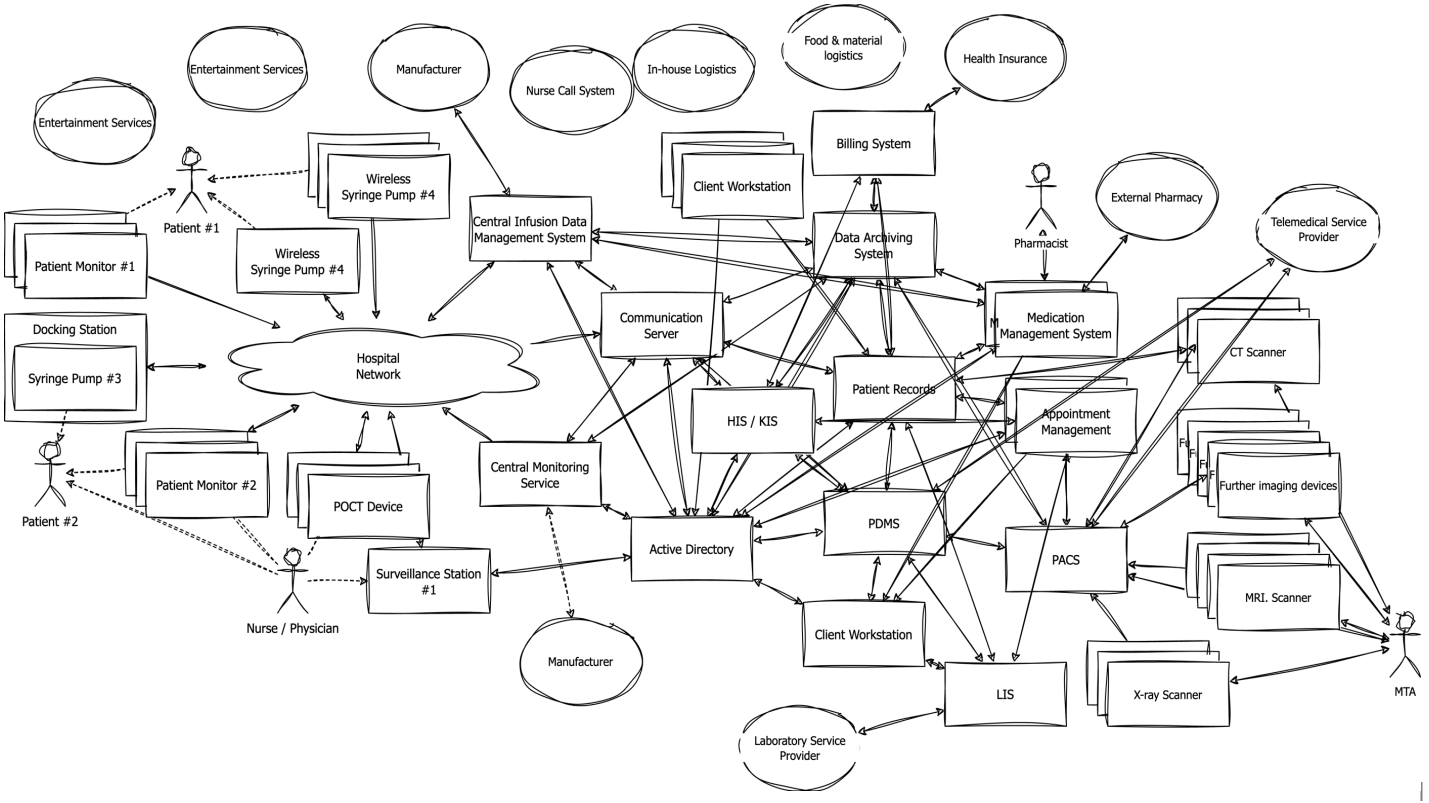
ERNW
providing security.



Standards

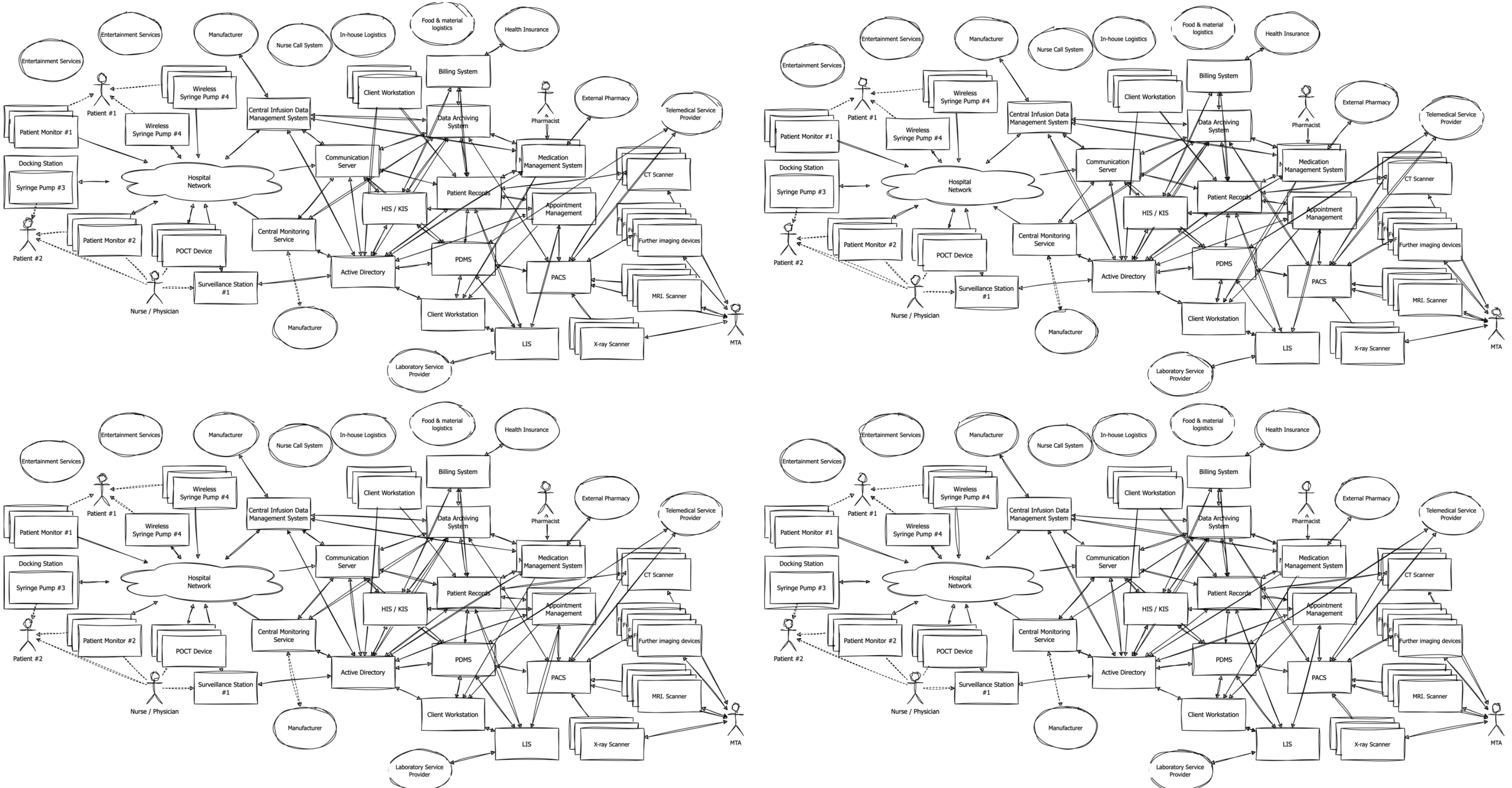
- Use predefinded standards, add you own and promote them to you suppliers!
- Be hard on them & limit exceptions
- Define clinic-wide standards
  - The same standards for all sizes of clincs
  - mesure them
  - rate them
  - execute them

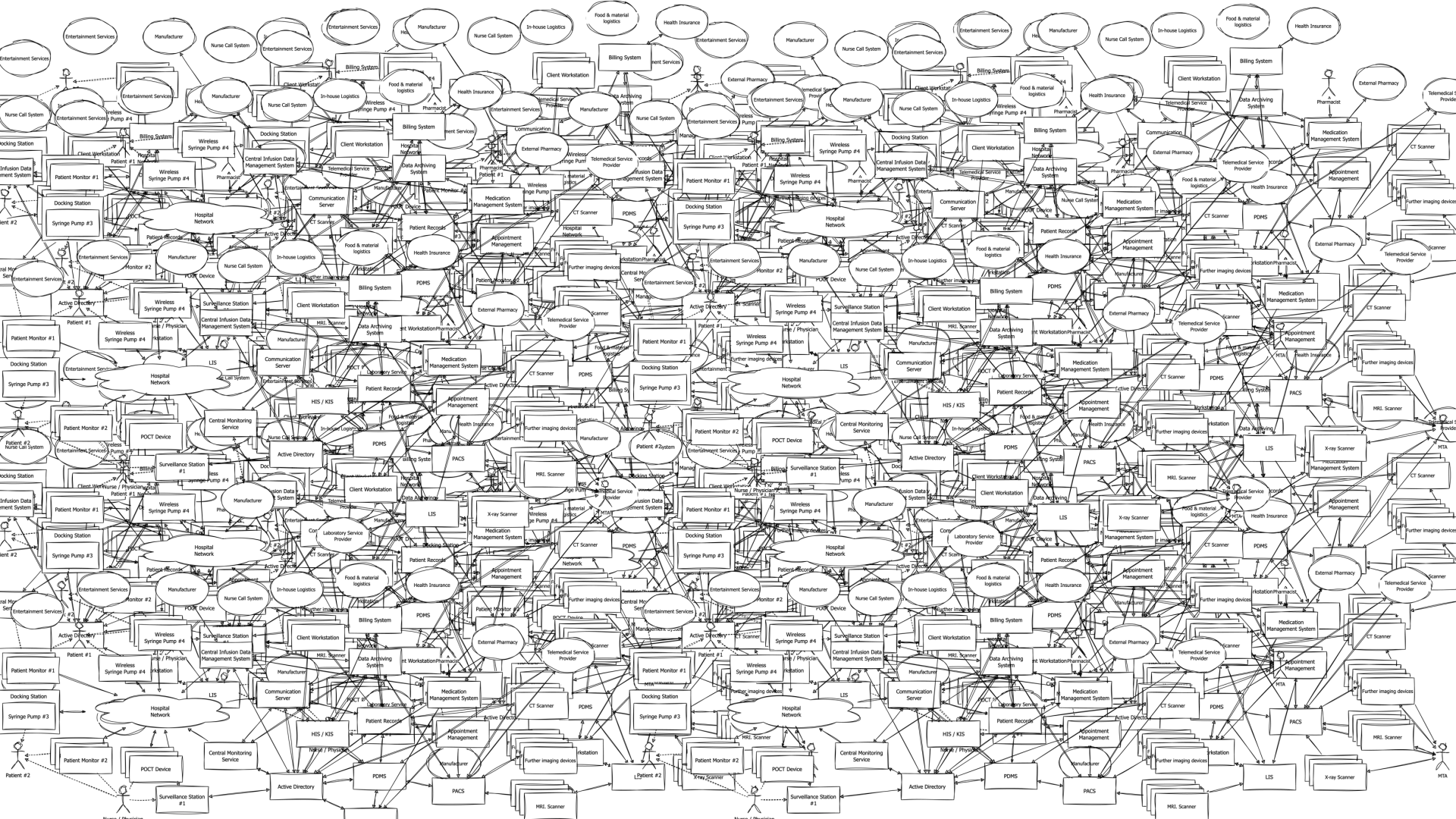
Our Exemplary Hospital …

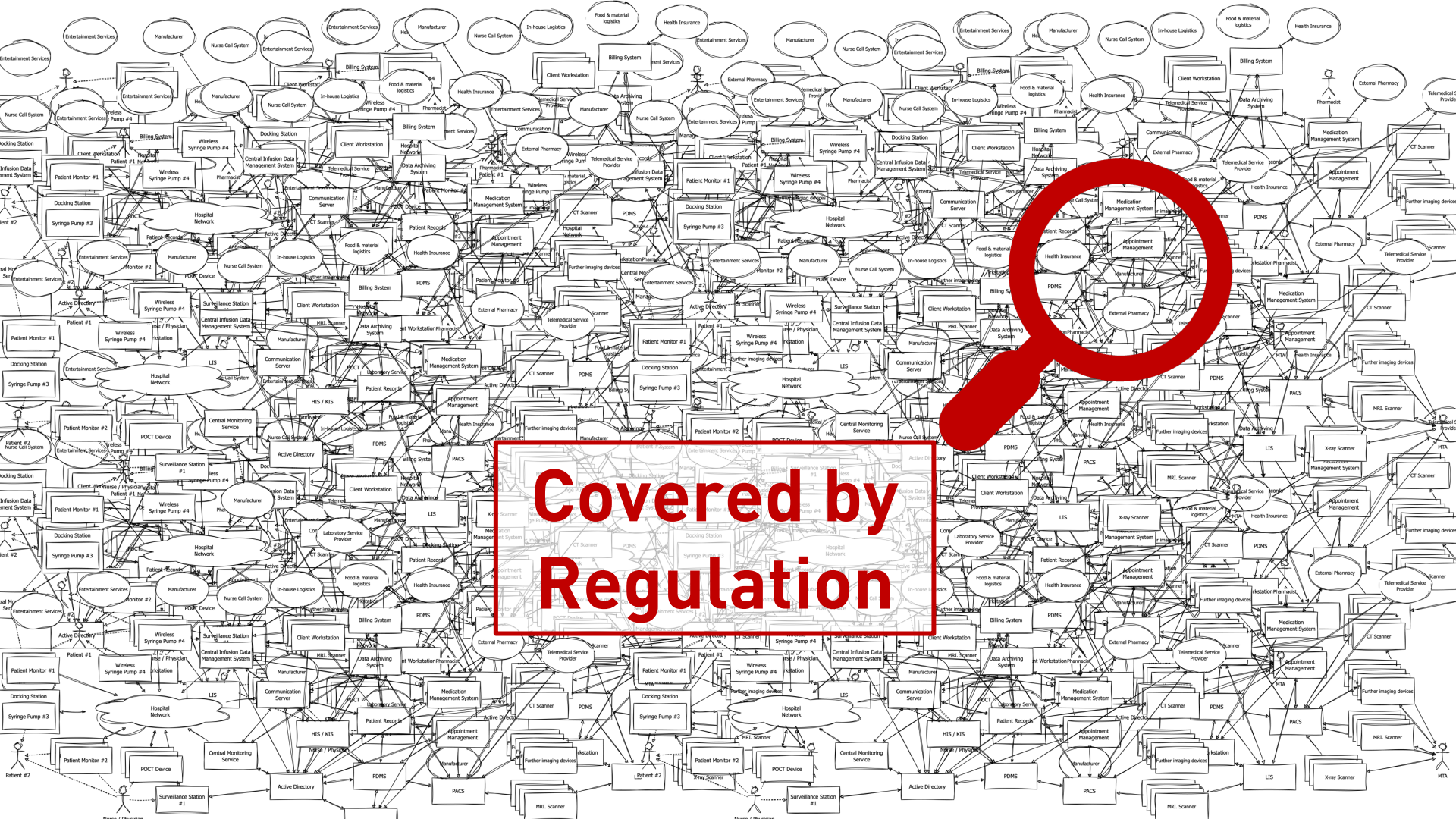


ERNW
providing security.

Our Exemplary Hospital ...




Entertainment Services
Manufacturer
Nurse Call System
In-house Logistics
Food & material logistics
Health Insurance
Billing System
Client Workstation
External Pharmacy
Pharmacist
Telemedical Service Provider
Data Archiving System
Wireless Syringe Pump #4
Docking Station
Syringe Pump #3
Patient Monitor #1
Central Infusion Data Management System
Communication Server
Medication Management System
Hospital Network
Patient Records
Appointment Management
CT Scanner
PDMS
Further imaging devices
Patient Monitor #2
POCT Device
Active Directory
Surveillance Station #1
Nurse / Physician
Patient #1
Patient #2
LIS
HIS / KIS
Central Monitoring Service
PACS
MRI Scanner
X-ray Scanner
MTA


Covered by Regulation

ERNW
providing security.

Next Steps?

ERNW
providing security.

IT & Operational Strategy

- Goal: Use human resources efficiently to operate the core infrastructure, while allowing facility-specific customization
  - → Define your security standards & processes
  - → Clear responsibilities, observability and regular assessment
  - → Require manufacturers to fit their products to your standards

ERNW
providing security.

Next Steps?

- There are new standards (HL7 FHIR, SDC, …) on a functional level
- Community engagement is crucial for future developments
  - Technical standardization for infrastructure integration
  - Technical guidelines by e.g. BSI → roadmap to legislation
- Use funding and development programs → Follow-up financing!

Thank you for your Attention!

https://www.linkedin.com/in/peterhecko
https://www.linkedin.com/in/juliansuleder

@heckpiet
@jsuleder

www.ernw.de

www.insinuator.net