voith.com

VOITH

CODE 2023 – Workshop 5
Cyber-Range-Trainings Wasserkraftwerke

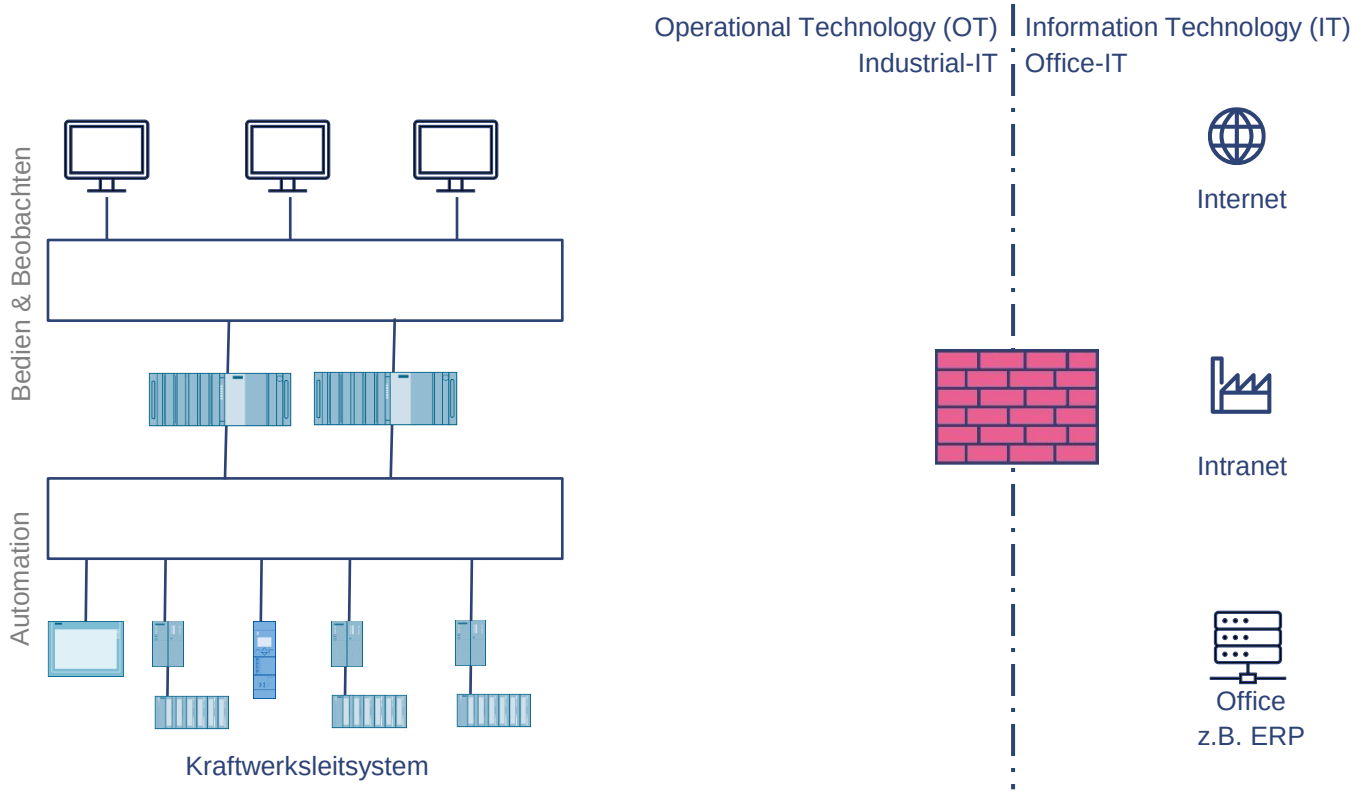
Heinz Marien | 2023-07-12

Kritische Infrastruktur
Wasserkraftwerke

Erzeugungskapazität bis zu 22 GW

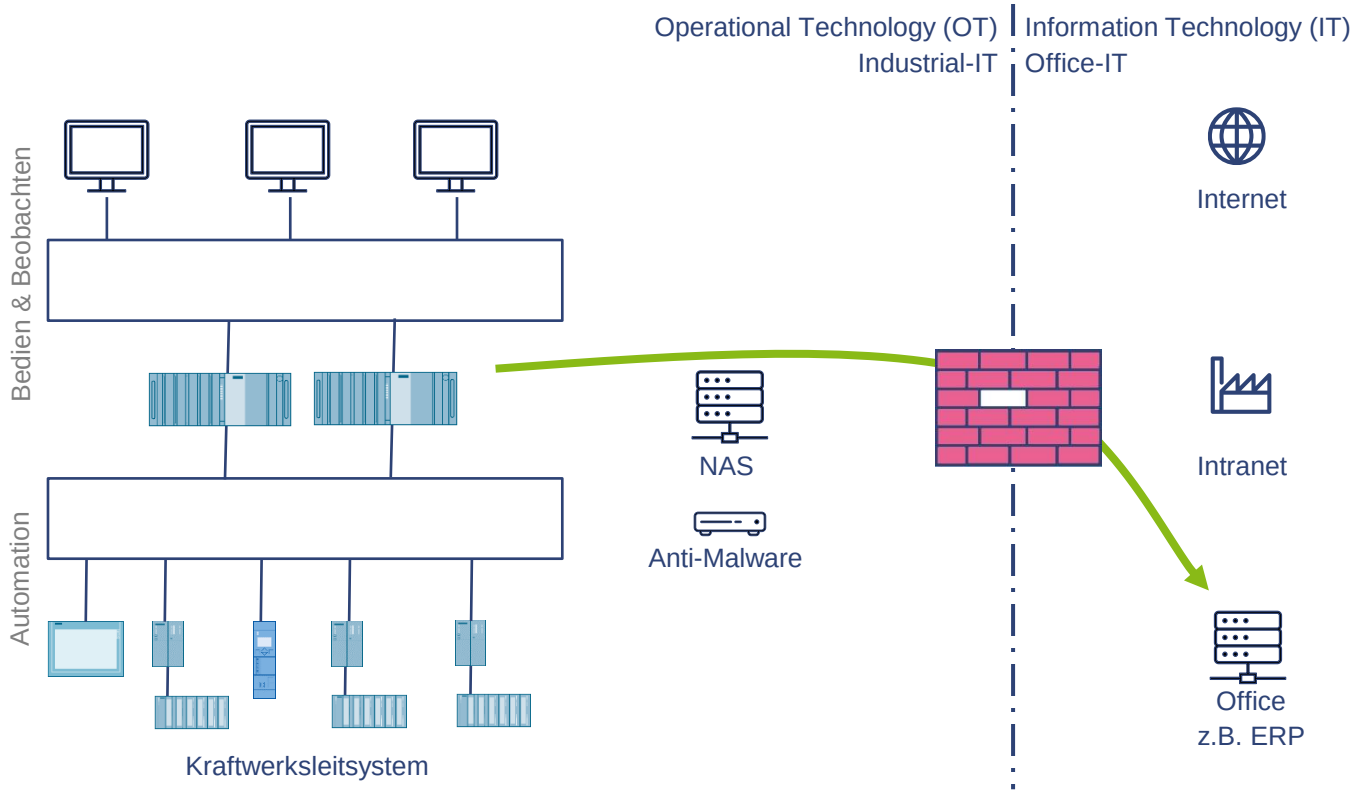
- Elektrische Energie für bis zu 100 Millionen Personen
- Vergleichbar zu
  - 4400 Wind Turbinen
  - 15 Thermischen Kraftwerken

Operational Technology Kraftwerke
System Architektur anno 2000



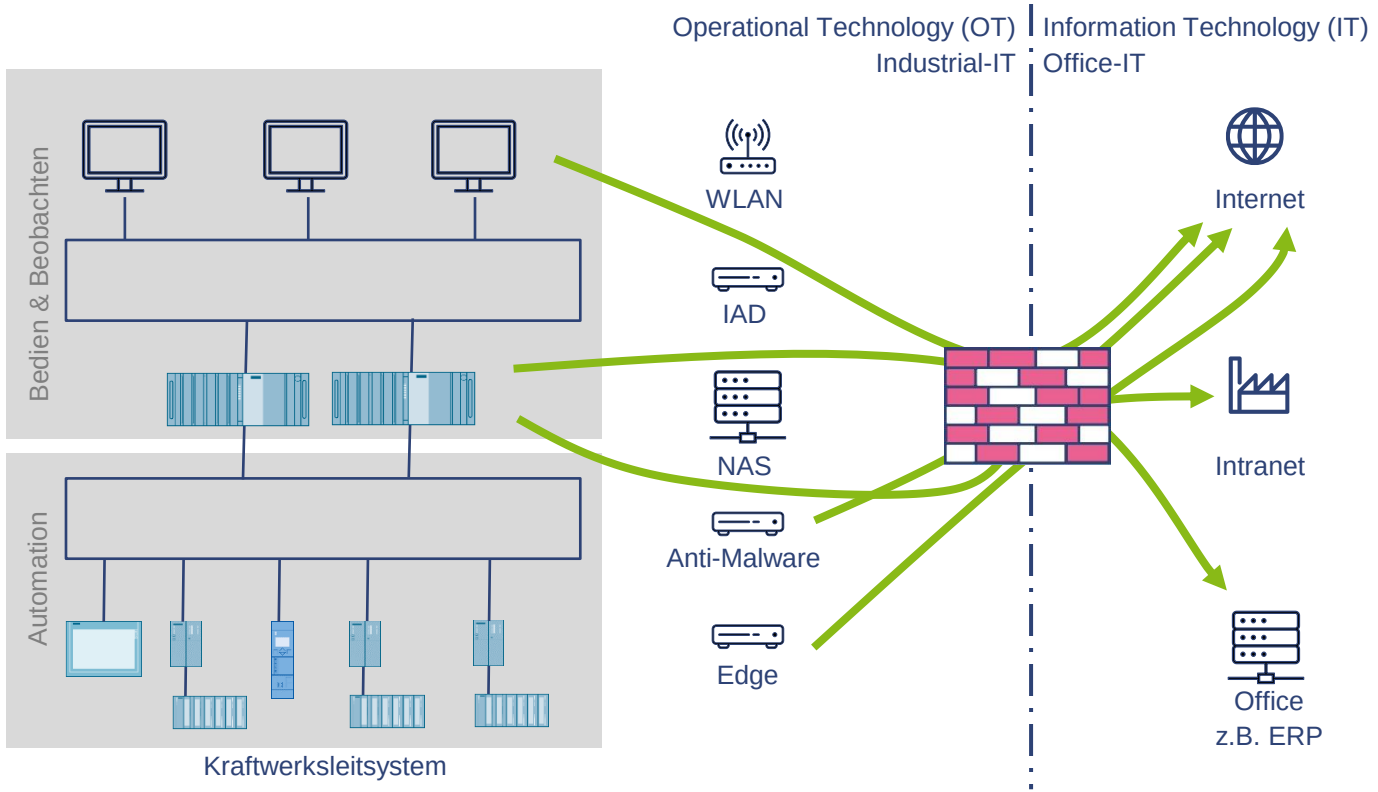
- „Air Gap“/ Insel-Architektur
- Vokabel „Security“ nicht existent
  keine Security Controls
- Lebenszyklus 15 Jahre
- Wartung/Betrieb durch lokales OT Personal
  „Never touch a running system“

Operational Technology Kraftwerke
System Architektur anno 2010



- Vernetzte Architektur
- Lebenszyklus 15 Jahre
- Wartung/Betrieb durch lokales OT Personal **„Never touch a running system“**
- **„1 Stück Firewall“** um die IT vor der OT zu schützen
- Anti-Malware Tools ohne Updates (Kostenoptimierung)

Operational Technology Kraftwerke
System Architektur anno 2020



- Vernetzte Architektur mit Zonen
- Lebenszyklus 15 Jahre
- Wartung/Betrieb durch lokales OT Personal **„1-2 Patch Termine / Jahr“**
- Internet Zugang für Remote Service, Patch/Updates, Cloud Services, etc.

Operational Technology Kraftwerke
System Architektur anno 20XX

Technische Maßnahmen

- Stärkere Vernetzung erzeugt **neue** Bedrohungen, welche Cyber Security (Überwachungs-) Anforderungen treiben.
- Eine Maßnahme alleine (z.B. Firewall) ist **nicht** mehr ausreichend, Ergänzung durch z.B. Angriffserkennungssystem (IDS).
- Durch IT/OT Konvergenz stehen in der OT **zukünftig** Konzepte wie Zero Trust zur Verfügung.

Konsequenzen

- Steigende **Komplexität** der System Architektur
- Steigende **Anforderungen** an Wartungs- & Betriebspersonal
- Parallel zur Prozessüberwachung muss auch die Cyber Security **kontinuierlich** überwacht werden. Hierdurch sind zusätzliche Qualifikationen notwendig.

Operational Technology Kraftwerke
Konflikt Lebenszyklus - Betriebssystem

Lebenszyklus Betriebssystem

0 Jahre	~ 2 Jahre	10 Jahre	15 Jahre
Neue Produkt Version	**Produkt Freigabe für KRITIS**	**Produkt Ende** • Keine Security Updates und Informationen	**Kein Support** • Keine Security Updates und Informationen

Lebenszyklus installiertes Kraftwerksleitsystem

Training für Widerstandsfähigkeit
Cyber Security Vorfalls Planung

VOITH

- Vorbeugung
  - Asset Management, Lieferanten-/Dienstleister-Management
  - Software Stückliste (SBOM)
  - Schwachstellenüberwachung, Patchmanagement
- Erkennung
  - Zuverlässiges Erkennung von „Angriffen“ durch Anlagen Überwachung (z.B. Protokollierungen, IDS , SIEM)
- Eindämmung/Behebung
  - Notfall-Maßnahmen

Vielen Dank!
Thank you!

Kontakt:
Heinz Marien
heinz.marien@voith.com

VOITH