L4-Appliance für Innere Suche

VeSiKi-Jahreskonferenz 2016, Bremen

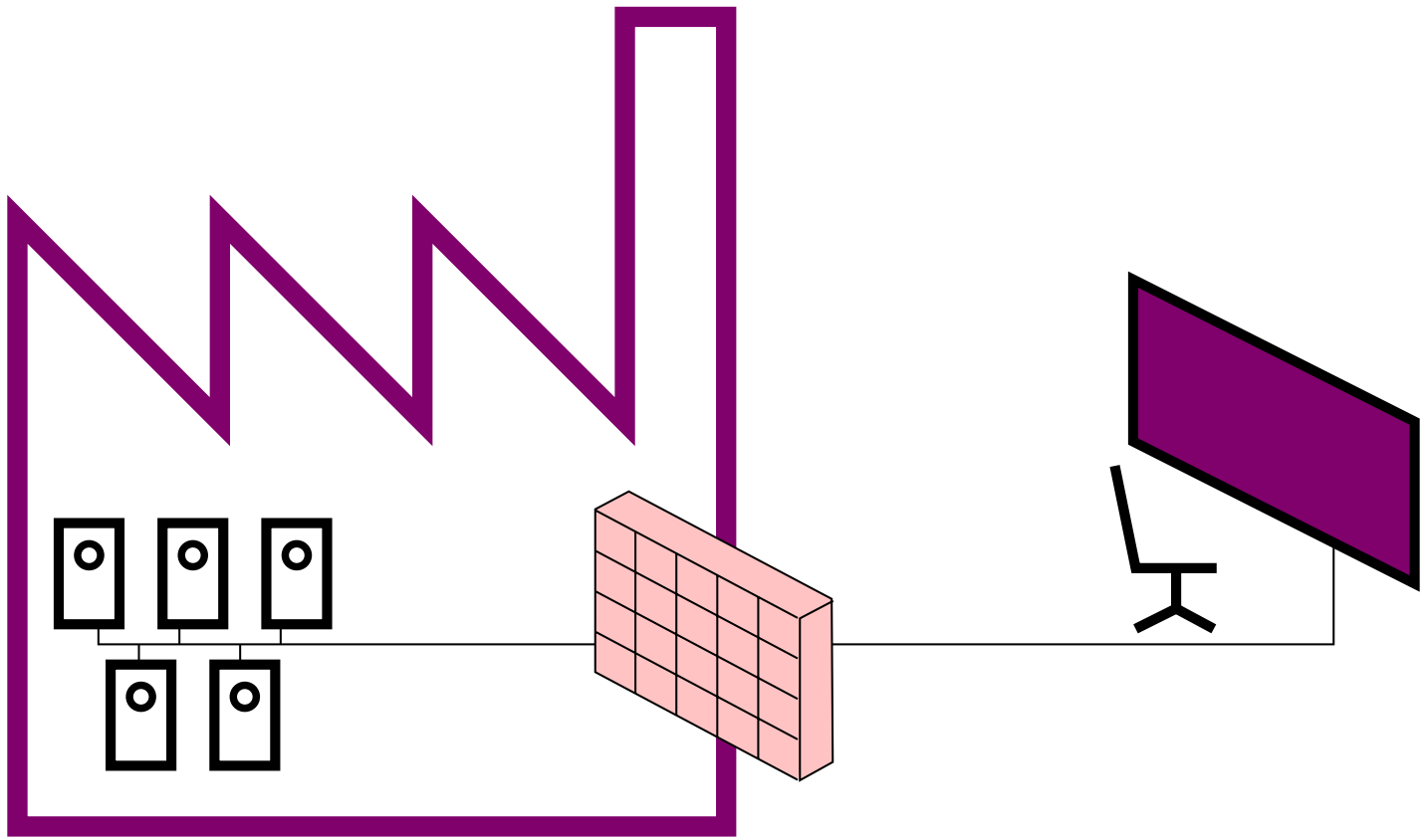
Christoph Moder

genua gmbh

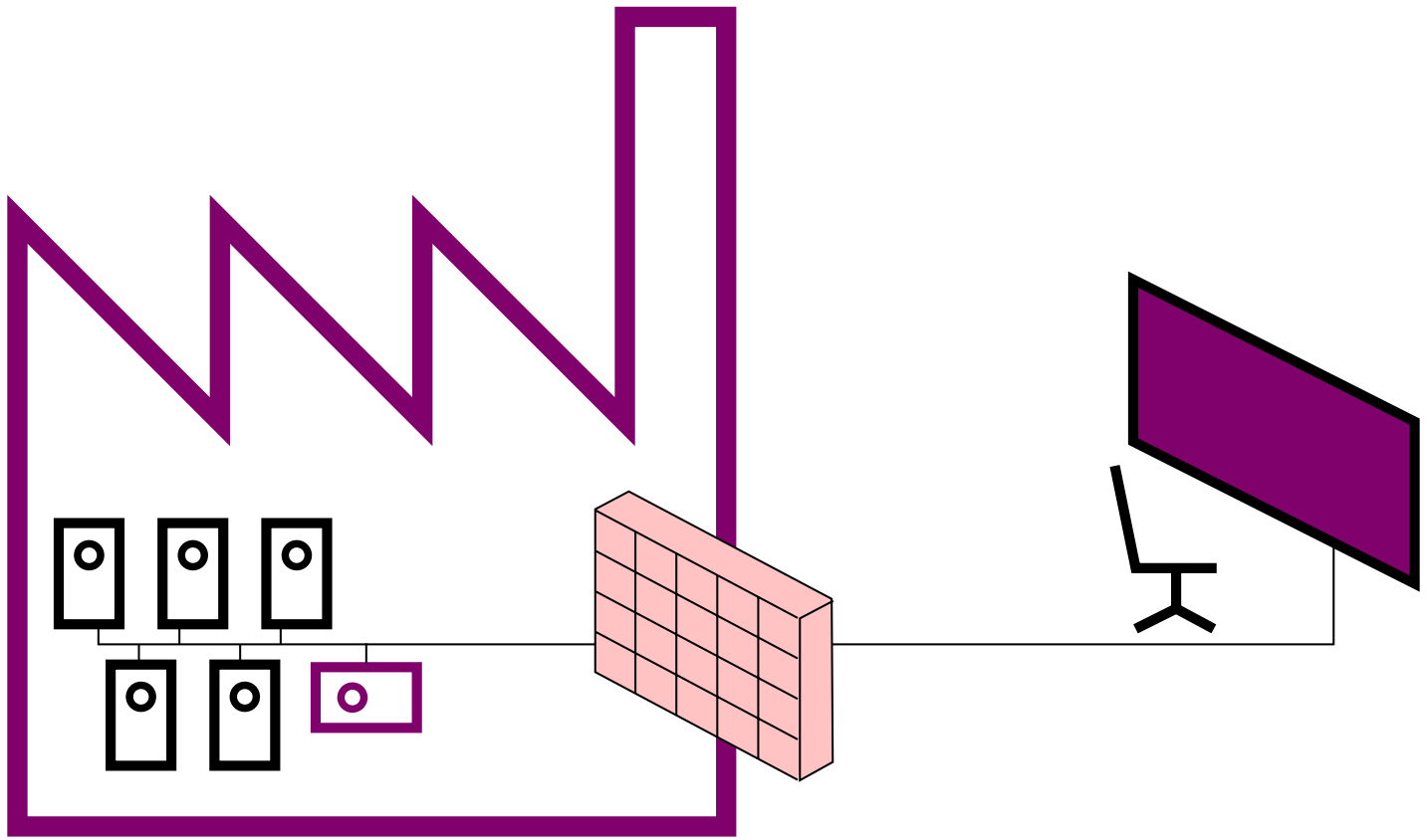
Christoph_Moder@genua.de

2016-06-21

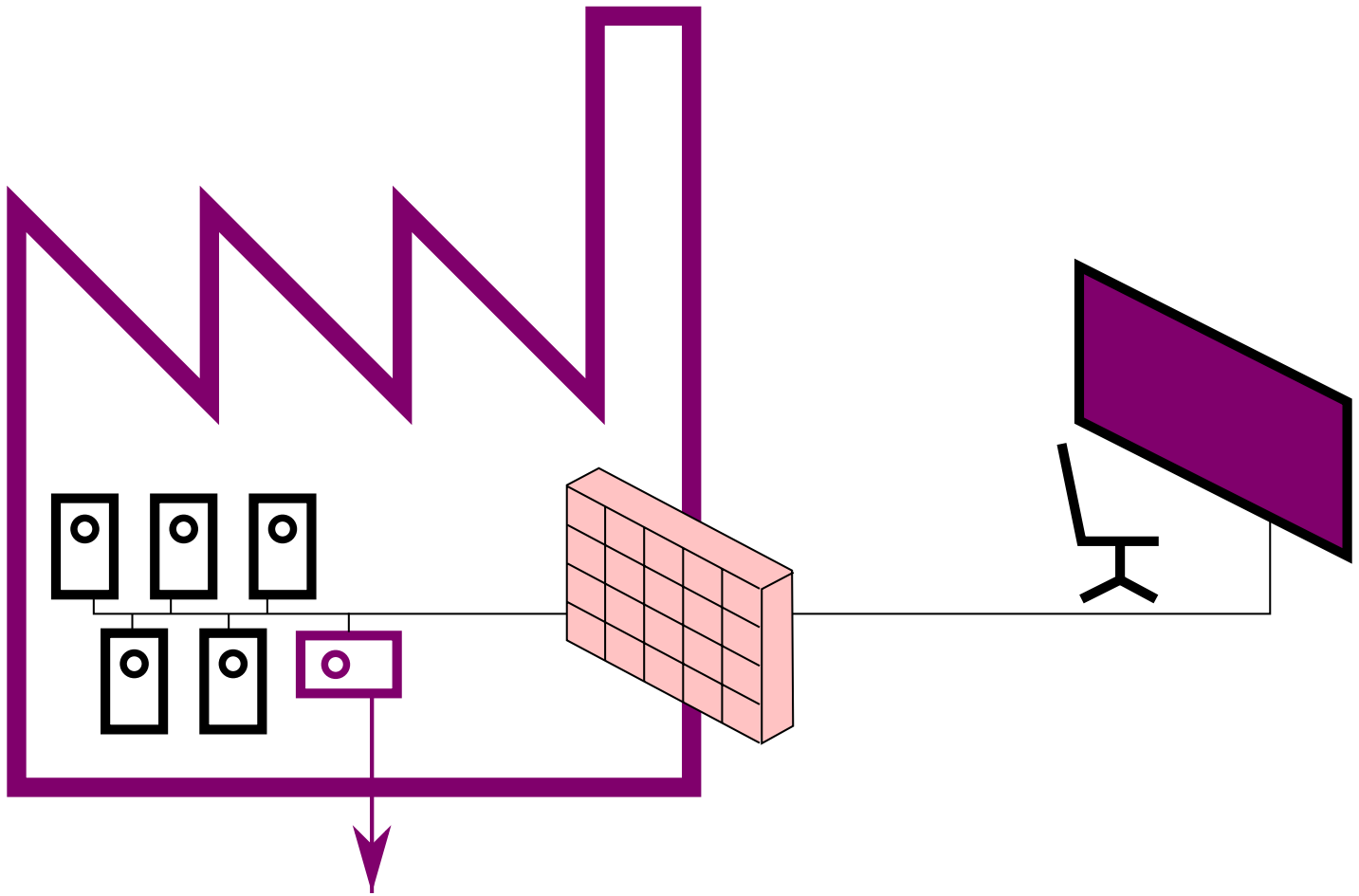
Aufgabe: Überwachung von Industriesteuerungen



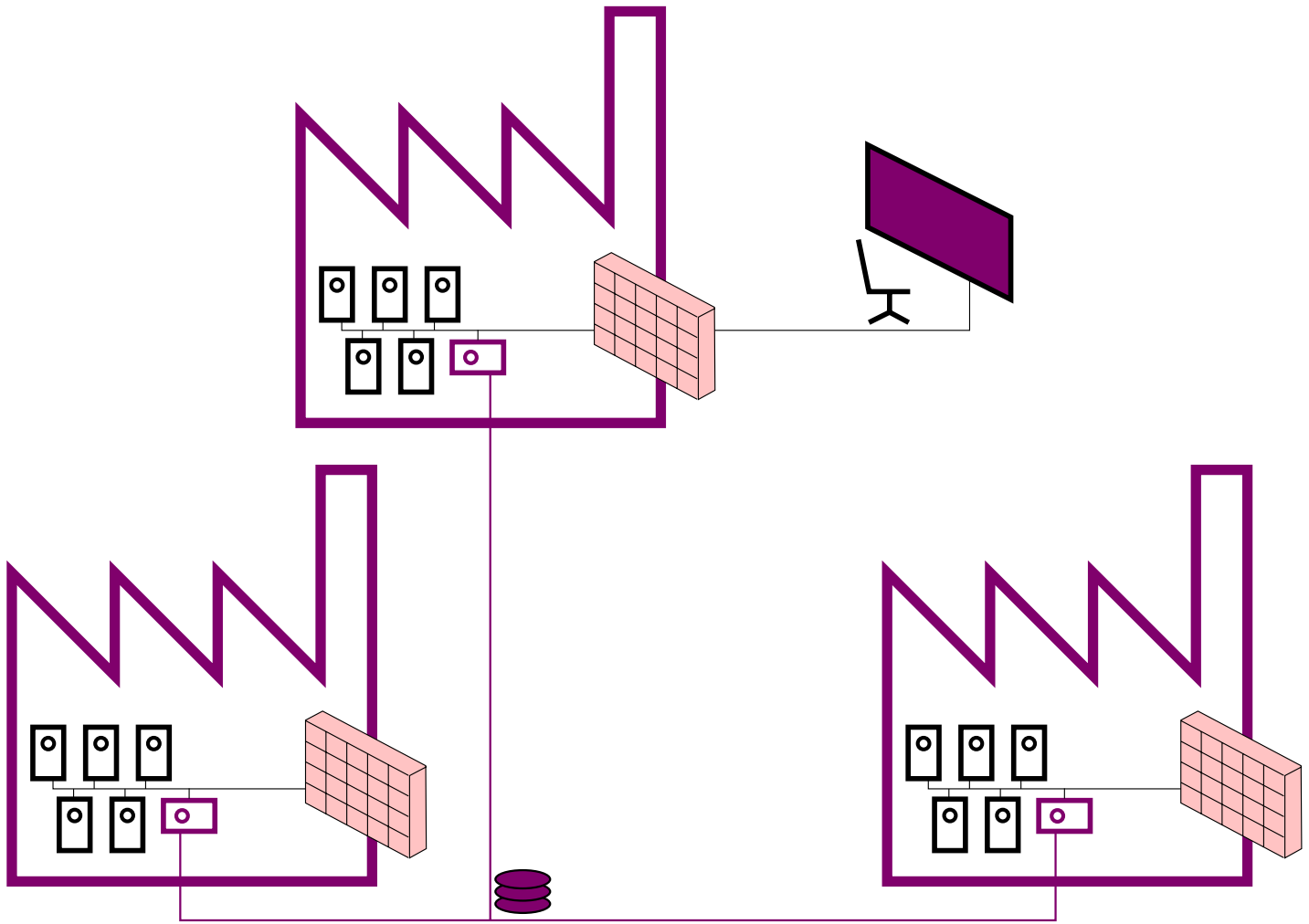
Einsatzort: innerhalb der Anlage



Anbindung an Kontrollzentrum

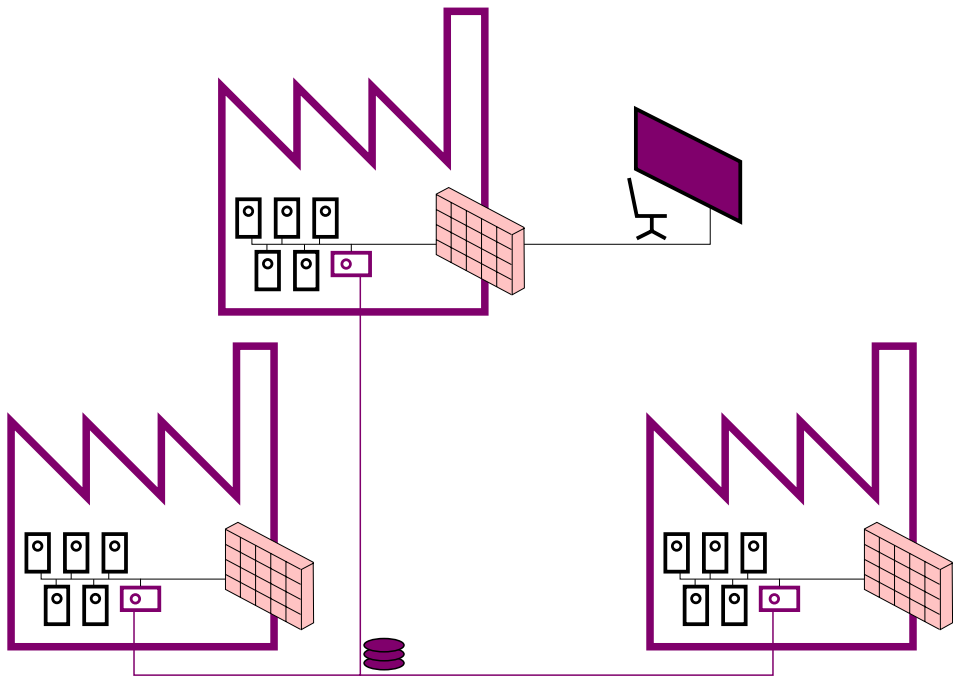


Anbindung an Kontrollzentrum



Anforderungen

- Anlagennetz scannen
- Kommunikation mit PLC
- Daten für Abruf bereit halten
- Mehrwert für Betreiber



Sicherheit

- kein Wirt für Schadcode

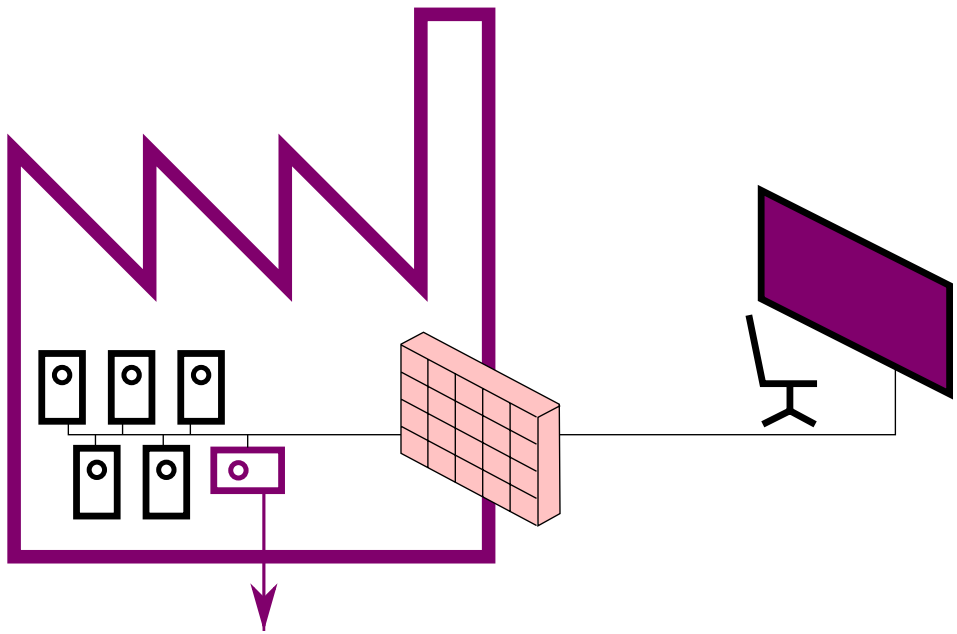
  ⇒ Sandboxing

- kein DoS durch Fehlfunktion

  ⇒ Datenfluss limitieren

- Netztrennung

  ⇒ Einweg-Datenverkehr



L4-Appliance: Überblick

- Zotac ZBOX CI521 nano
- CPU: Intel Core M
- 2 Ethernet-NICs
- L4-Microkernel
- L4Linux/L4OpenBSD

Was ist ein Microkernel?

- nur Basisfunktionen:

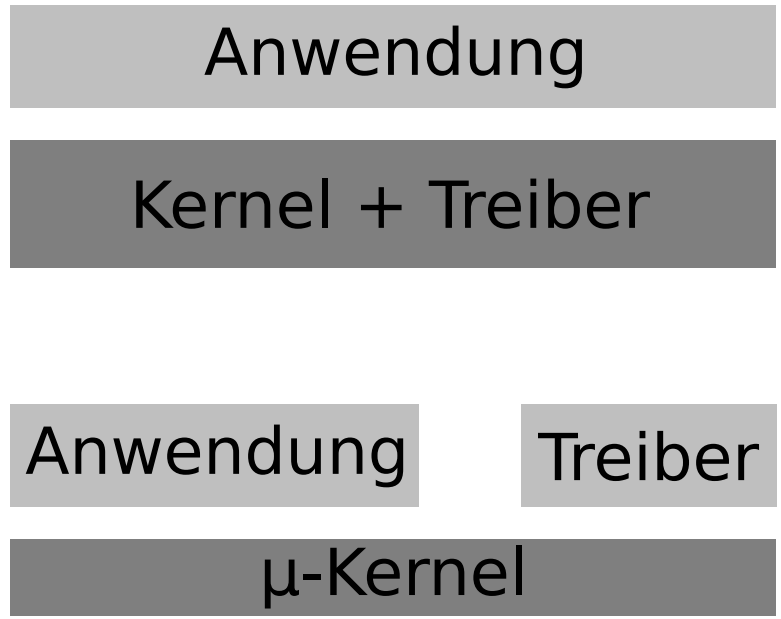
  Rechenzeit, Speicherschutz

- Kommunikation zwischen Tasks

- kleine *Trusted Computing Base*

  ($\approx$ Faktor 100 kleiner)

- Funktionalität in Userspace

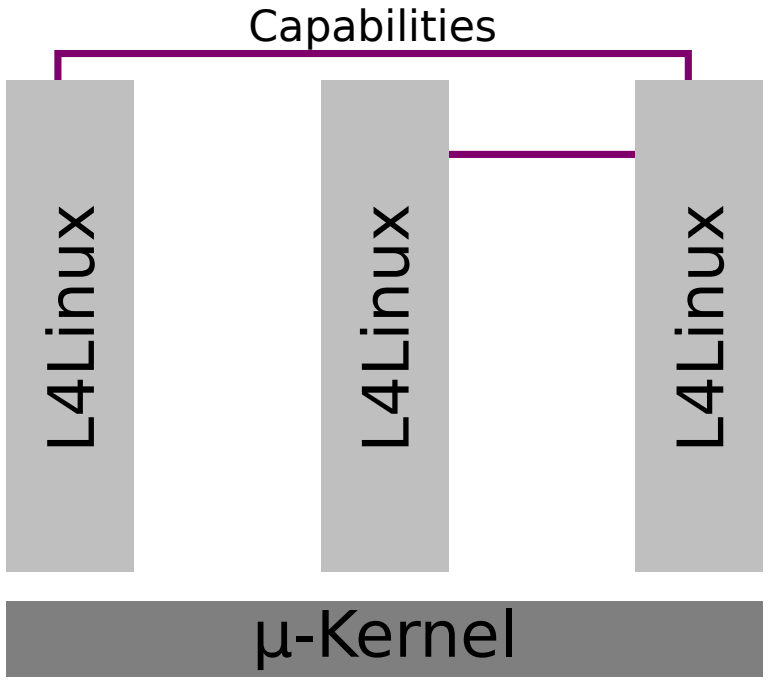


L4 Fiasco.OC

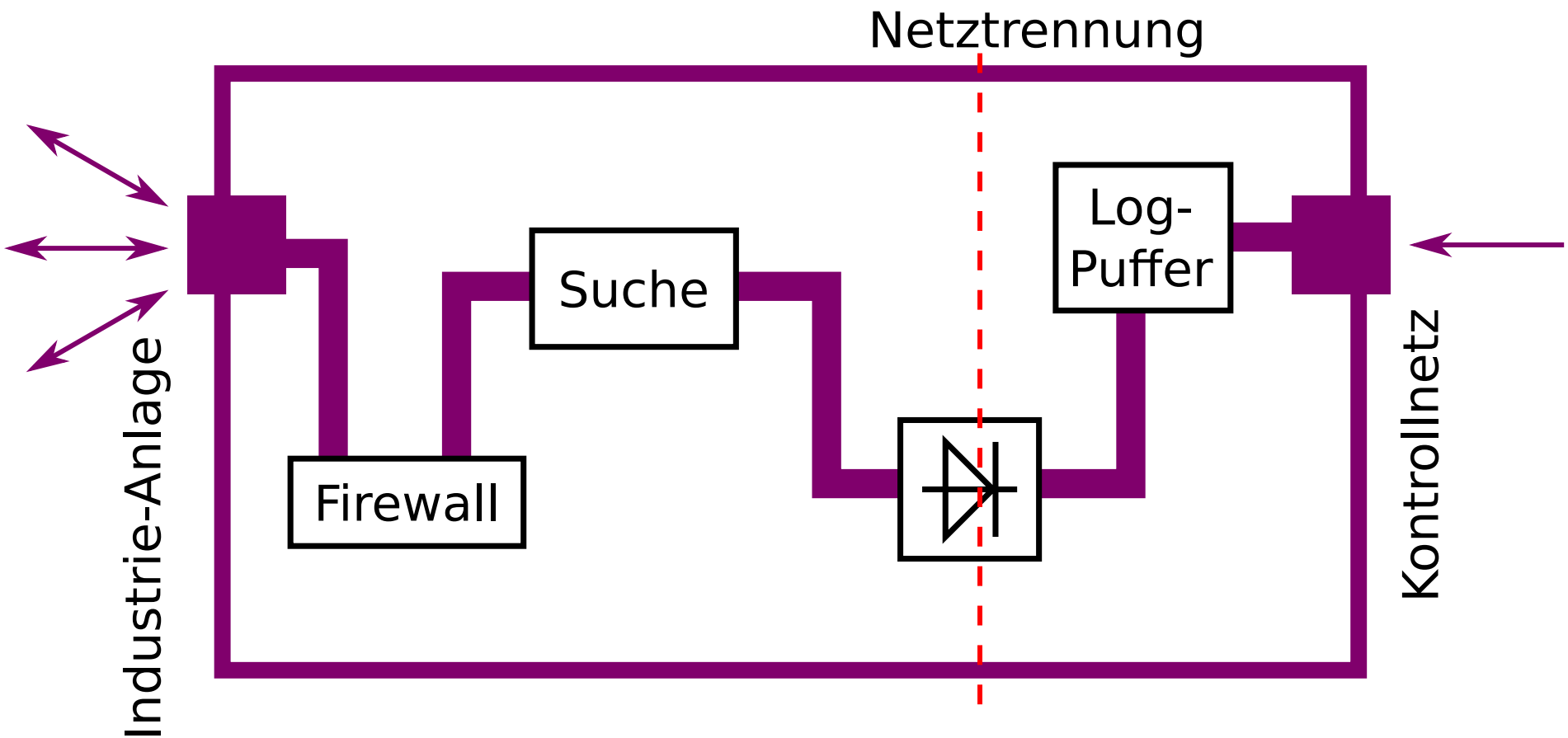
- L4-Familie = Jochen Liedtke
- Fiasco.OC:

  TU Dresden; Kernkonzept
- Object Capabilities:

  Whitelisting von Datenflüssen
- Hardware exklusiv an Task
- paravirtualisiertes Linux/OpenBSD



L4-Appliance

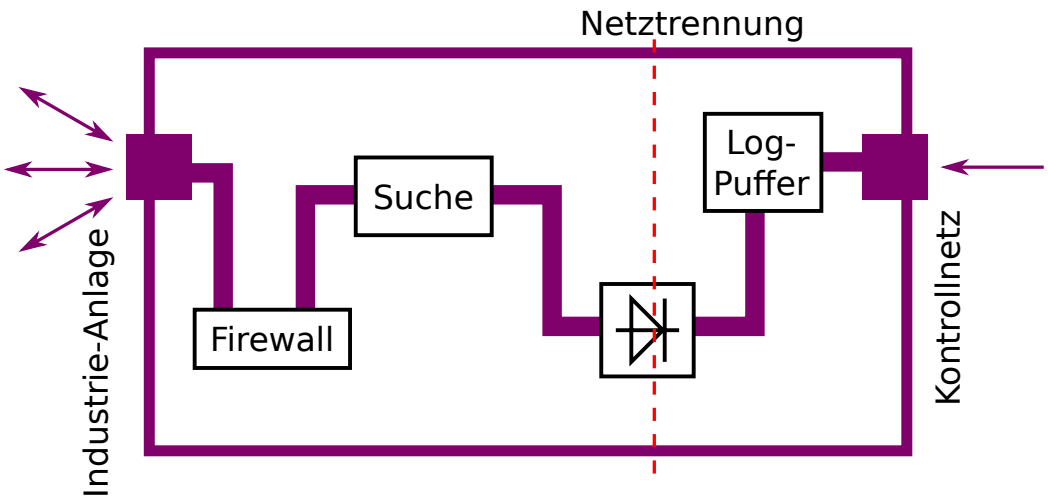


L4-Appliance

- Innere Suche
- Firewall:

  regelt Datenrate
- Diode:

  Einweg-Kommunikation
- Log-Puffer: Abholung



Zusammenfassung

- Industrieanlagen-Überwachung von innen
- L4: Abschottung von Prozessen

  ⇒ Aufteilung in Compartments
- L4: Whitelisting von Datenfluss

  ⇒ Kontrolle der Kommunikationskanäle
- Dioden-Task

  ⇒ Netztrennung, Einweg-Datenverkehr

Zusammenfassung

- Industrieanlagen-Überwachung von innen
- L4: Abschottung von Prozessen

  ⇒ Aufteilung in Compartments
- L4: Whitelisting von Datenfluss

  ⇒ Kontrolle der Kommunikationskanäle
- Dioden-Task

  ⇒ Netztrennung, Einweg-Datenverkehr

Danke!