When Safety meets Security

Dr. Magnus Harlander
genua GmbH
Munich - November 2016

Who is genua?

- Specialist for TOP-IT-Security
- German company
- Founded in 1992
- 52% shares at Bundesdruckerei
- Located in Munich
- Offices in Berlin, Cologne, Stuttgart
- 230 employes, including 15% apprentices
- genufix: company run by our trainees for social organizations
- genukids: Kinderhaus for 30 kids

BUNDES DRUCKEREI

Our Markets

German and international High-Security-Markets

- Government und public Sector
- Defense and Security
- Industry and Plant Construction
- Critical Infrastructures
- Hidden Champions
- Fortune 500

Industry now digitalized

- Many possible scenarios
  - Network connections between IT and OT
  - Remote access for maintenance
  - Predictive maintenance
  - Industrial bigdata
  - Industrial data space and cloud integration
  - M2M
  - IOT

=> There is a plug in the plant

This is a cultural clash!

- IT

  - Bugs accepted
  - Patch interval < 4 weeks
  - Volatile interfaces
  - Short innovation cycles
  - Complex implementations
  - Interconnecting everything
  - Certifications take years
  - Availability **first**
  - Security by management
  - Safety irrelevant

- OT

  - Bugs not acceptable
  - Uptime > 10 Jahre
  - Stable interfaces
  - Innovations in decades
  - Simple hard- und software
  - Local networking only
  - Runs after construction
  - Safety **first**
  - Safety by design
  - Security irrelevant

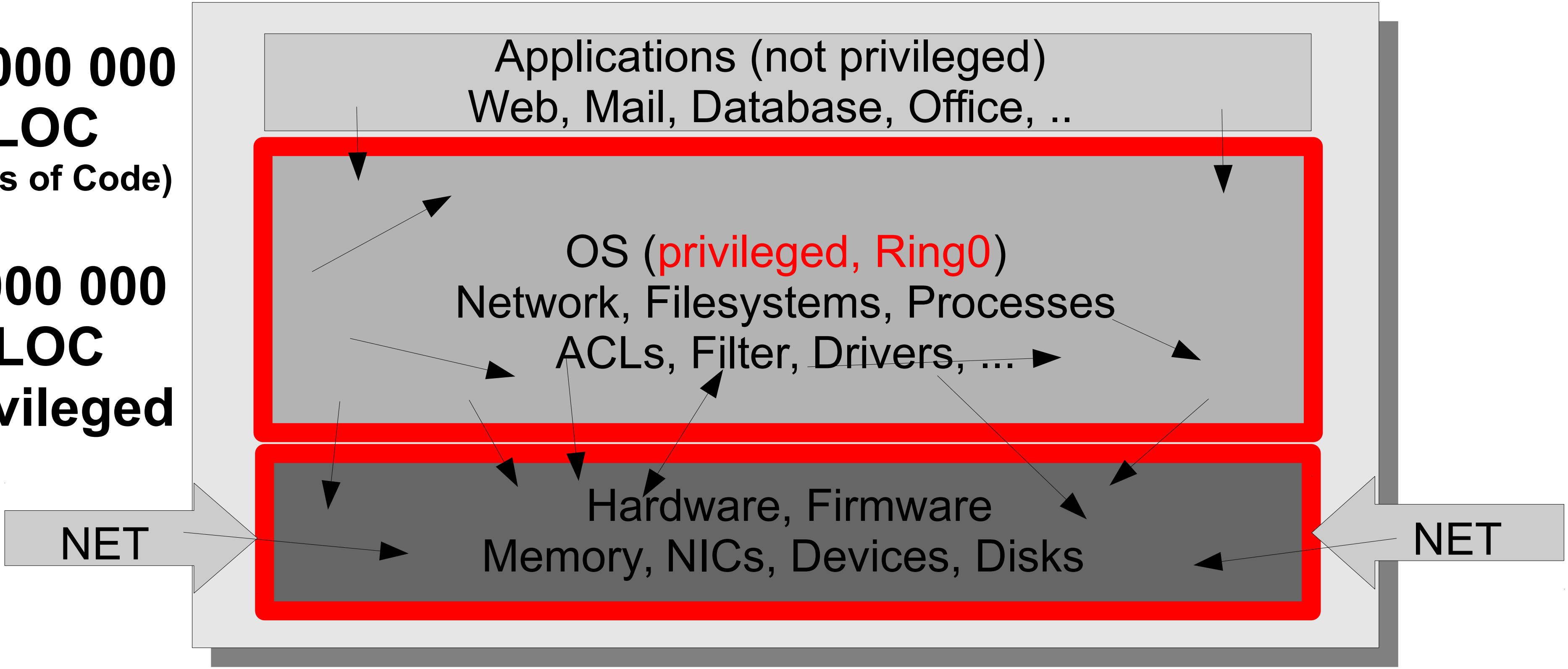
What IT must learn for OT?

- Learn to handle errors correctly / Plan B
  - Redundance
  - Resilience
- Keep the humans out
  - Security by design
  - Minimal administration and configuration needs
- Reduce connections and minimize systems
  - Create stable interfaces
  - Reduce complexity

Architecture of a *normal Security System*

50 000 000
LOC
(Lines of Code)

5 000 000
LOC
privileged



Applications (not privileged)
Web, Mail, Database, Office, ..

OS (privileged, Ring0)
Network, Filesystems, Processes
ACLs, Filter, Drivers, ...

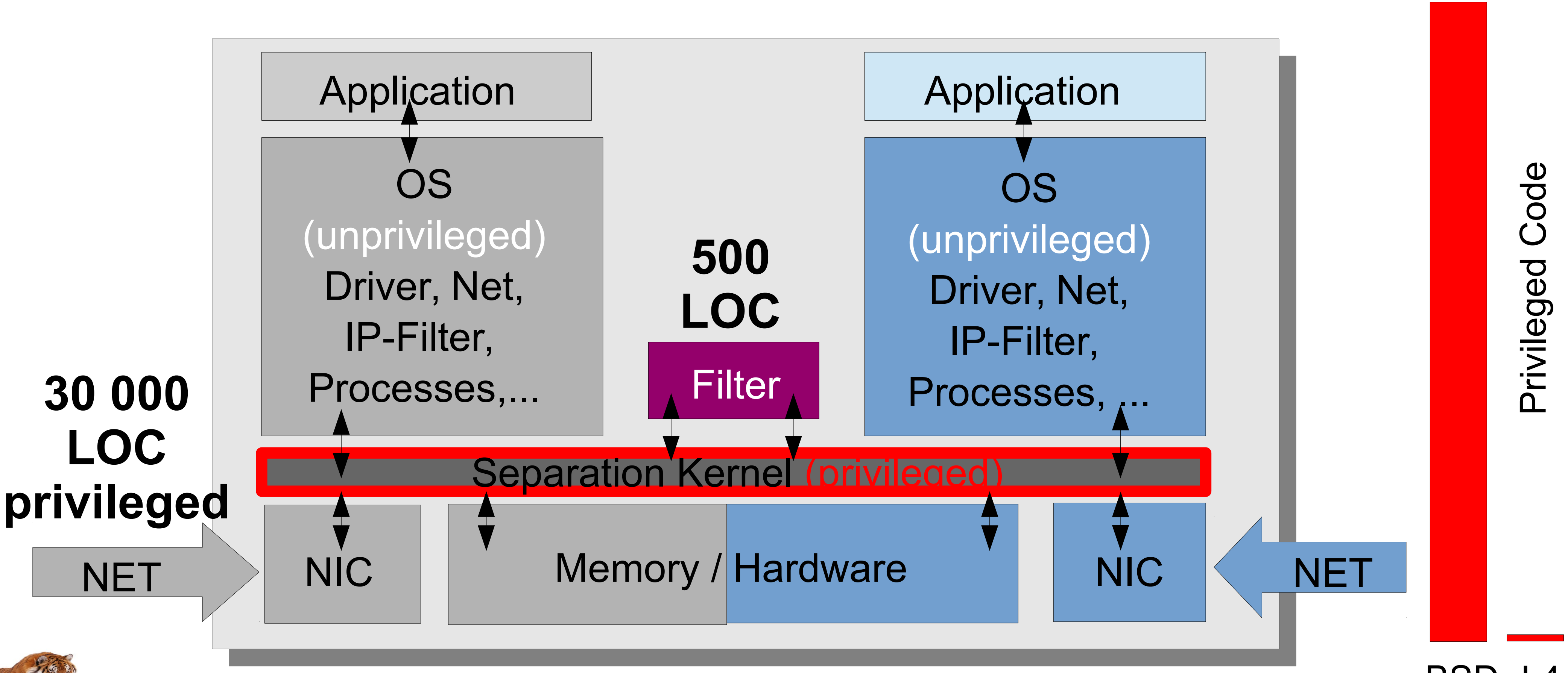
Hardware, Firmware
Memory, NICs, Devices, Disks

Windows, Linux, IOS, VX-Works, BSD, ...

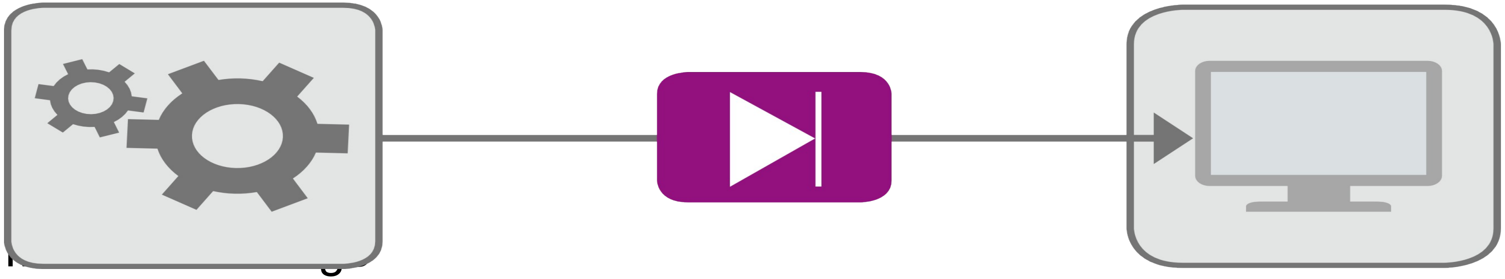
Minimal Systems

- Separate components
  - Software
  - Hardware
- Separate functionality
- Reduce number of interfaces
- Create simple interfaces
- Reduce privileged code base
- Reduce complexity

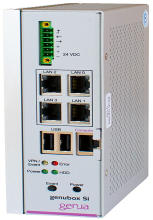
Architecture of a minimal Separation System



Example: Data Diode



Machine
Plan
PCS
Control room
Sensor network
...



SOC
Cloud
Bigdata
Monitoring
Data analysis
...

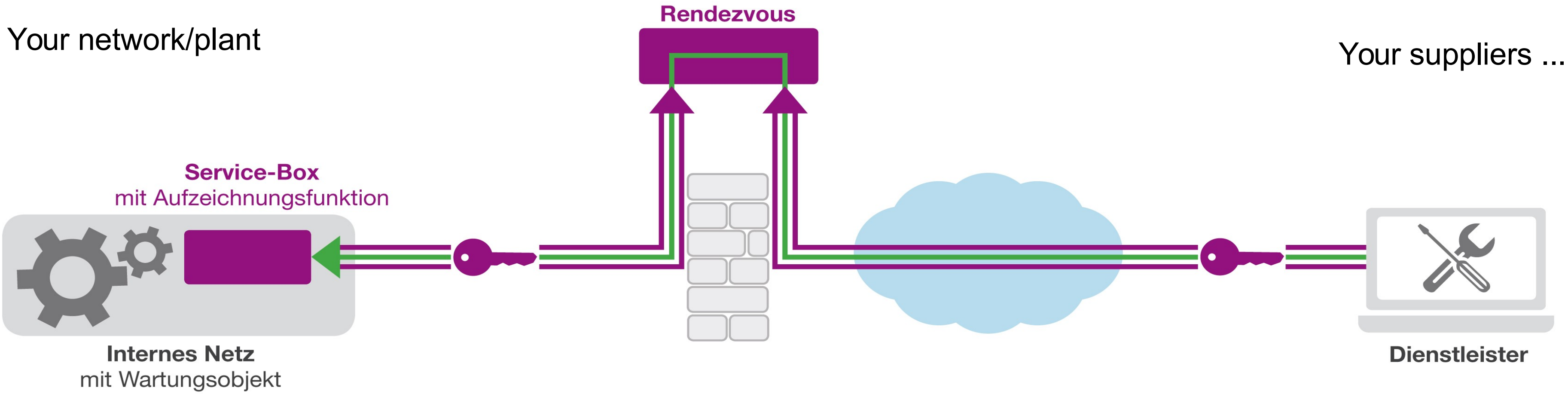
Data export without backlash

Remote Service using minimal Networking

- BSI recommendation for remote service:
  - One and only one solution
  - Use a DMZ
  - Don't use routing (not Layer 2/3 VPN)
  - Connection establishment always from the inside
  - Use dedicated systems
  - Use secure protocols and cryptographic algorithms
  - Strong authentication and strong passwords
  - Minimalization principle
  - Use limited time boxes
  - ....

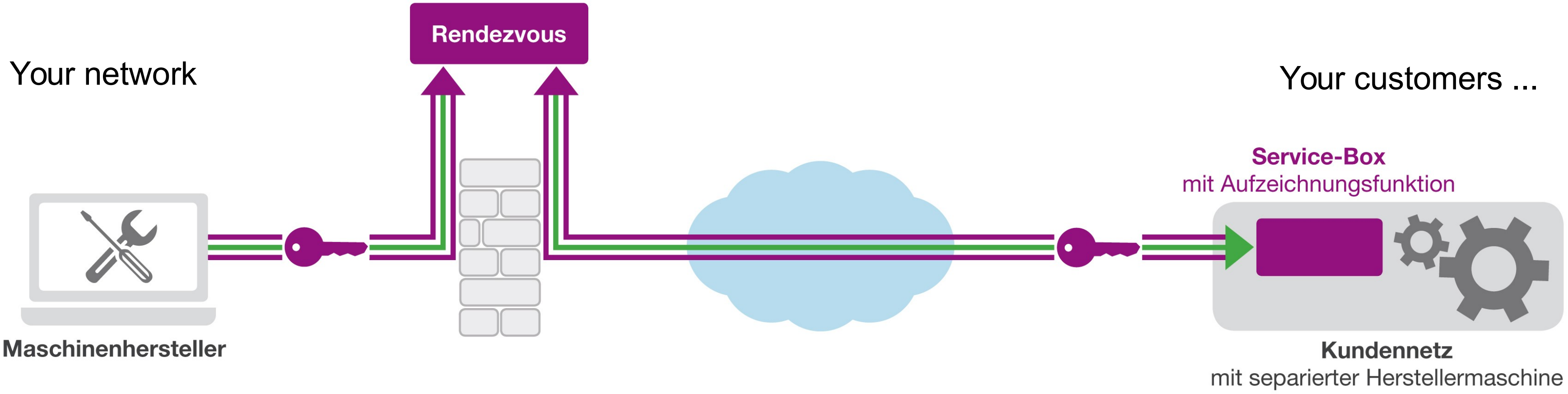
The Victims View

- We are all victims. IT and OT is affected
- Remove all your modems, DSL Routers, Wifi, VPNs, ...
- Almost no requirements for the suppliers
- Use SSH tunnels with proxies
- Two factor, session recording, live monitoring, ...



The Intruders View

- For machine and plant construction companies
- Management by the remote service provider
- Control is still on the customers side
- Minimal access to the customers network
- No hassle with the customers IT admins



Your network

Rendezvous

Your customers ...

Service-Box
mit Aufzeichnungsfunktion

Maschinenhersteller

Kundennetz
mit separierter Herstellermaschine

Summary

Keep it small and simple

Don't trust IT professionals over 30 (kLOC)

There will be the bug, that affects you

Always have a plan B for security breaches

Murphy is everywhere

magnus_harlander@genua.de