

When Safety meets Security



Dr. Magnus Harlander
genua gmbh
Munich - February 2017

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



German and international High-Security-Markets

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



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

=> There is a plug in the plant



.. 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

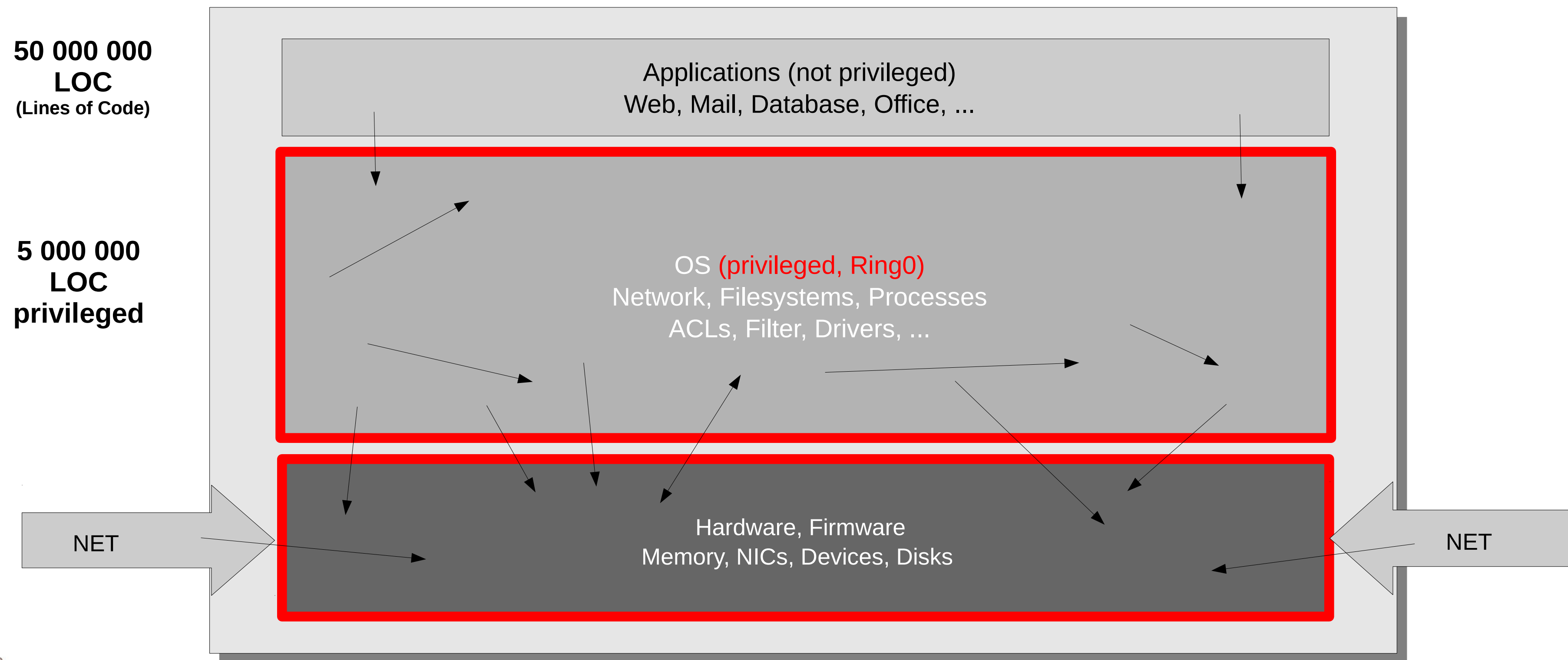


- .. Bugs not acceptable
- .. Uptime > 10 years
- .. Stable interfaces
- .. Innovations in decades
- .. Simple hard- und software
- .. Local networking only
- .. Runs after construction
- .. Safety **first**
- .. Safety by design
- .. Security irrelevant



- .. Learn to handle errors correctly / Plan B
 - .. Redundance
 - .. Resilience
 - .. Contain effects of security breaches
- .. Keep the humans out
 - .. Security by design
 - .. Minimal administration and configuration needs
- .. Reduce connections and minimize systems
 - .. Create stable interfaces
 - .. Reduce complexity
 - .. Reduce attack surface





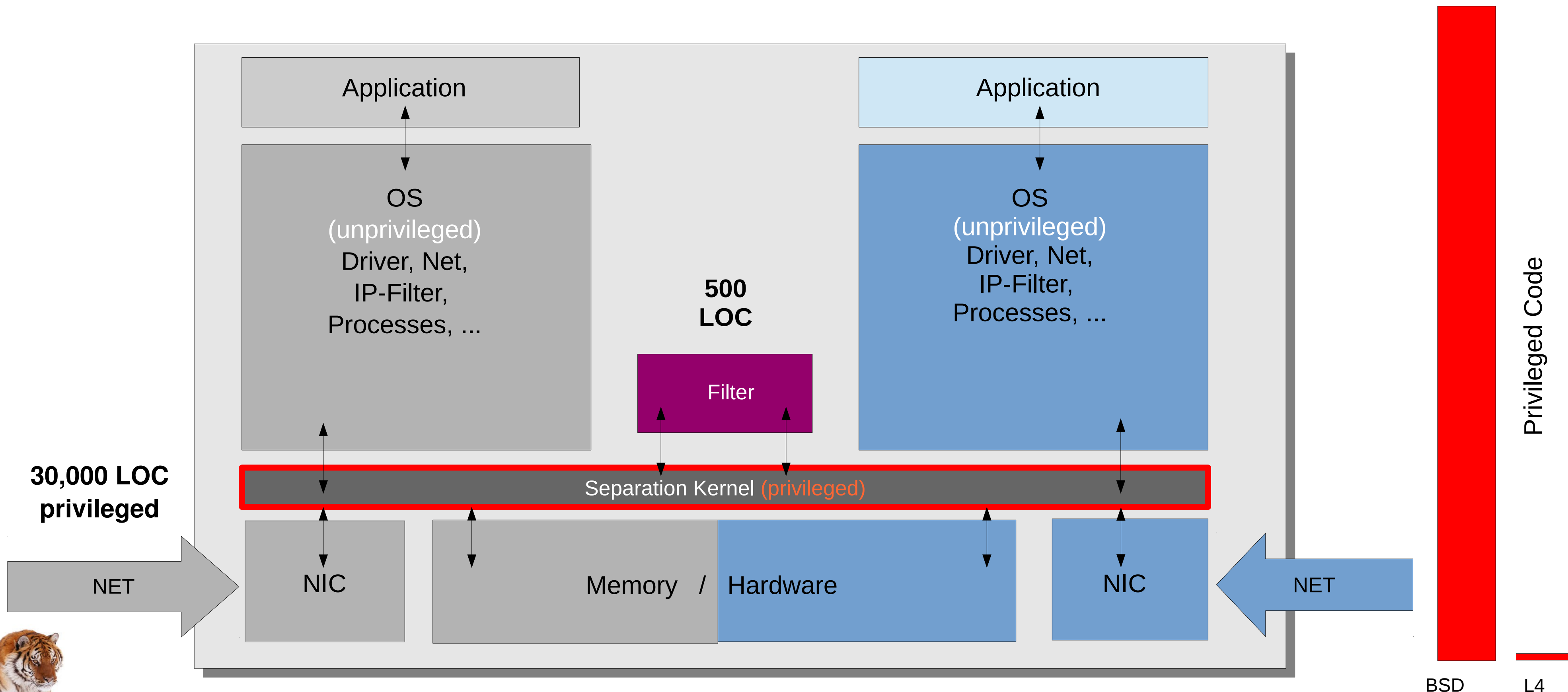
Windows, Linux, IOS, VX-Works, BSD, ...



- .. 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





Data export without backlash

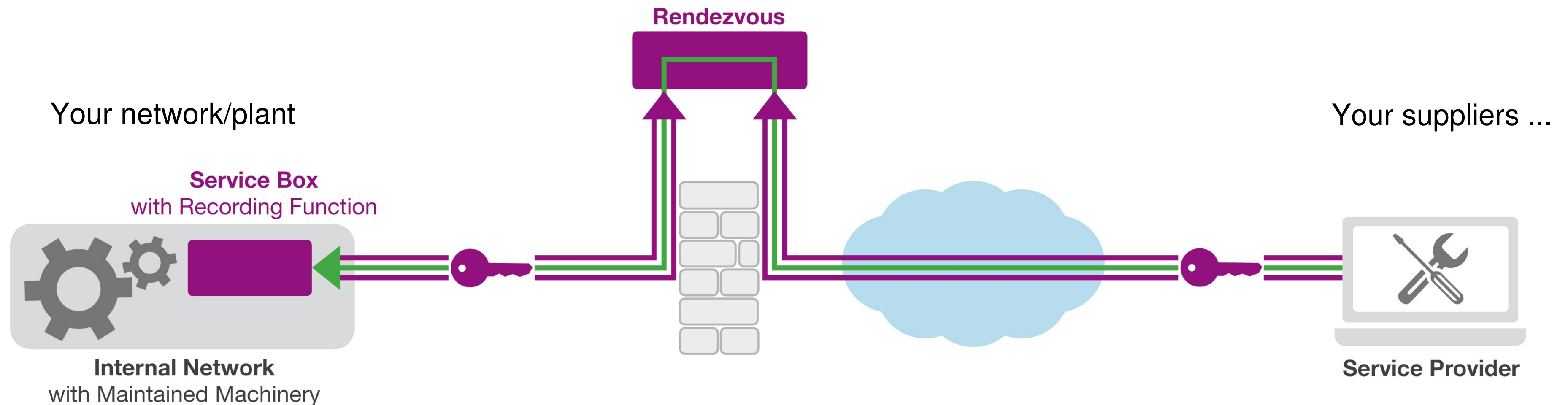


- .. BSI recommendation for remote service:
 - .. One and only one solution
 - .. Use a DMZ
 - .. Don't use routing (not Layer 2/3 VPN)
 - .. Connection establishment always from the inside
 - .. Use dedicated systems
 - .. Use secure protocols and cryptographic algorithms
 - .. Strong authentication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



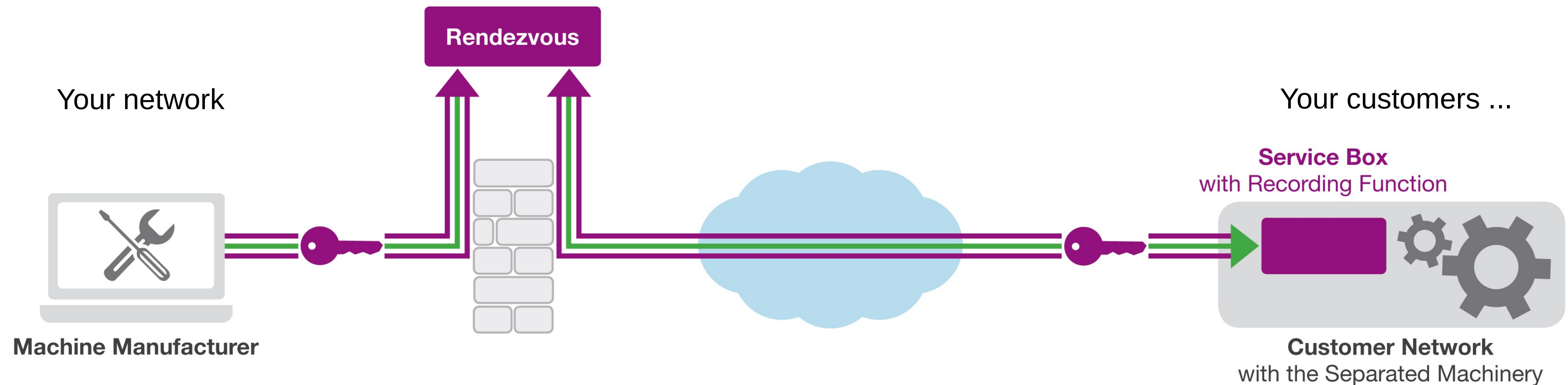
The Victims View

- 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



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

