Security 4.0 - Security by Separation

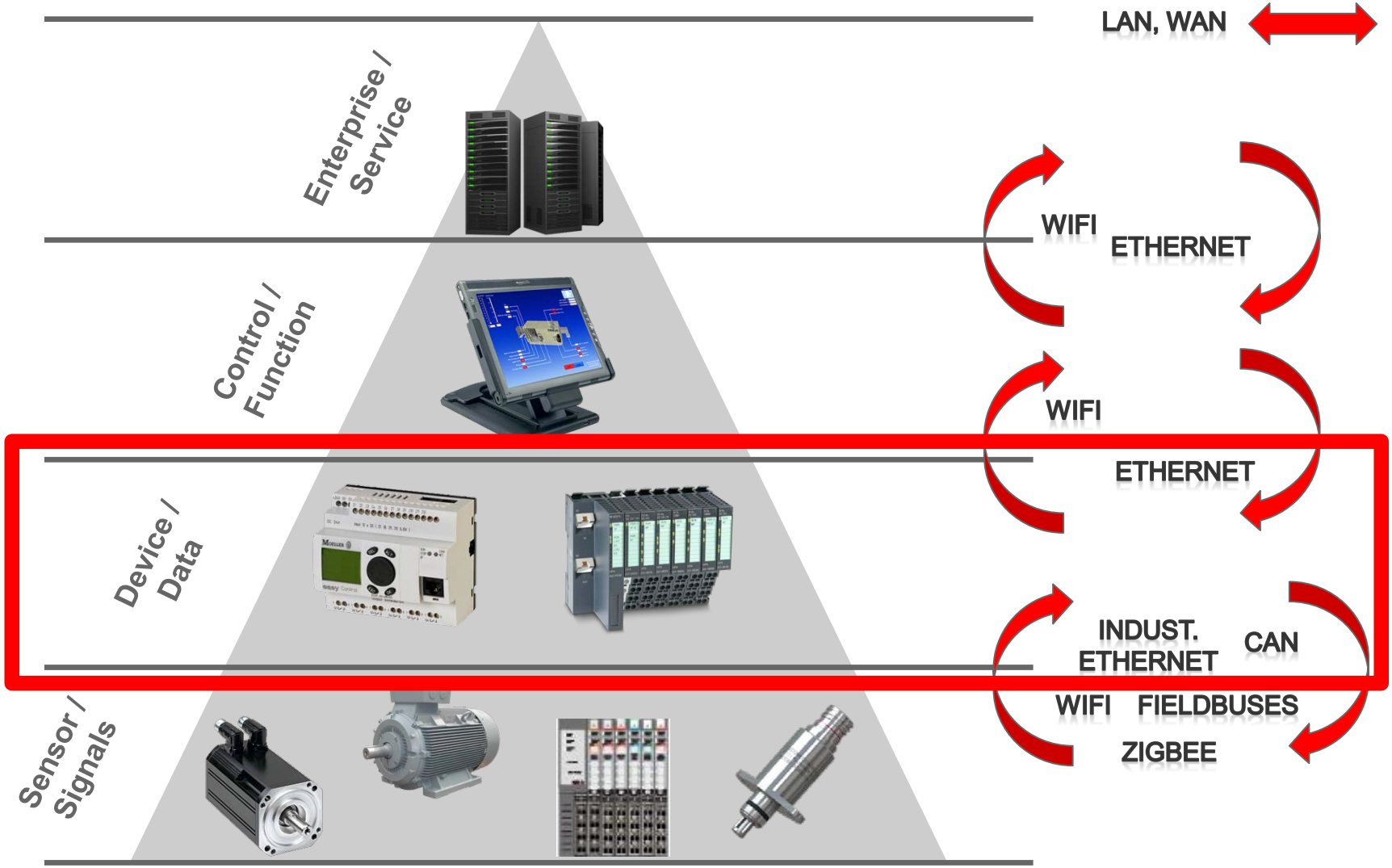
Making Industrial Control Systems More Secure

Author(s): Mehmet Özer
Date: 19.05.2015
Version v1.0

Agenda

- **Security Challenges**
  - IoT Architecture for Industrial Automation
  - Industrial Automation Security
- **Separation Kernel**
  - Separation Kernel Security Concept
  - Linux Security
- **Security Add-On**
  - Secure Boot
  - Policy Management
- **Security Certification**
  - Common Criteria EAL-X
- **Summary**

Information Flow – Industrial Control System (ICS)



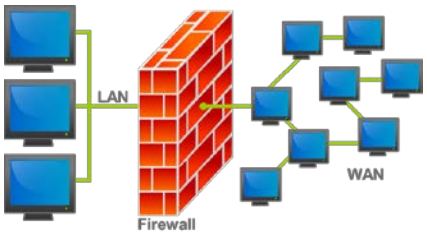
http://upload.wikimedia.org/wikipedia/commons/9/9c/Cylinders_with_Hall_sensors.png
http://www.automationworld.com/sites/default/files/styles/lightbox/public/field/image/1307np_vipa.png?itok=9QYZ4-VT
http://www.markbourgeois.com/portfolio/moeller usa_net/products/Automation/media/plc-hmi_plc.png
magazine.qualys.fr
http://static1.1.sqspcdn.com/static/f/614694/13935925/1314910419277/8GRTD100+PNG.png?token=hfpg%2BH6HIMyy%2Bj3GJKHTX4qrEdQ%3D

ICS Security Challenges

	Office - Devices	ICS - Devices
Handled Risks	Confidentiality of Data !!! Confidentiality !! Integrity ! Availability	Preserve Safety, Real-Time Execution and availability: !!! Availability !! Integrity ! Confidentiality
Security Means	- Commercial Solutions - Broadly used	- Availability for OS or architecture - Update policy
Updates / Patches /	- Update Server - Remote Access	- Do I loose my safety certification ? - Is Remote Access a Backdoor?
Maintenance	- Regularly	- 24/7 operation - Availability requires high up-time
Product Life-Cycle	- 2-4 years - Up to Date Hardware and Software	- 10 up to 30 years - Handle Obsolescence

Security by Separation – Network Security

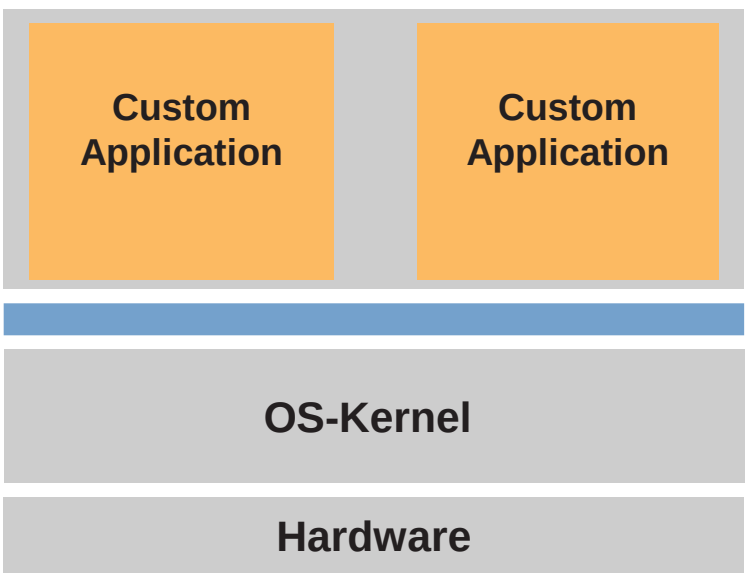
Firewall



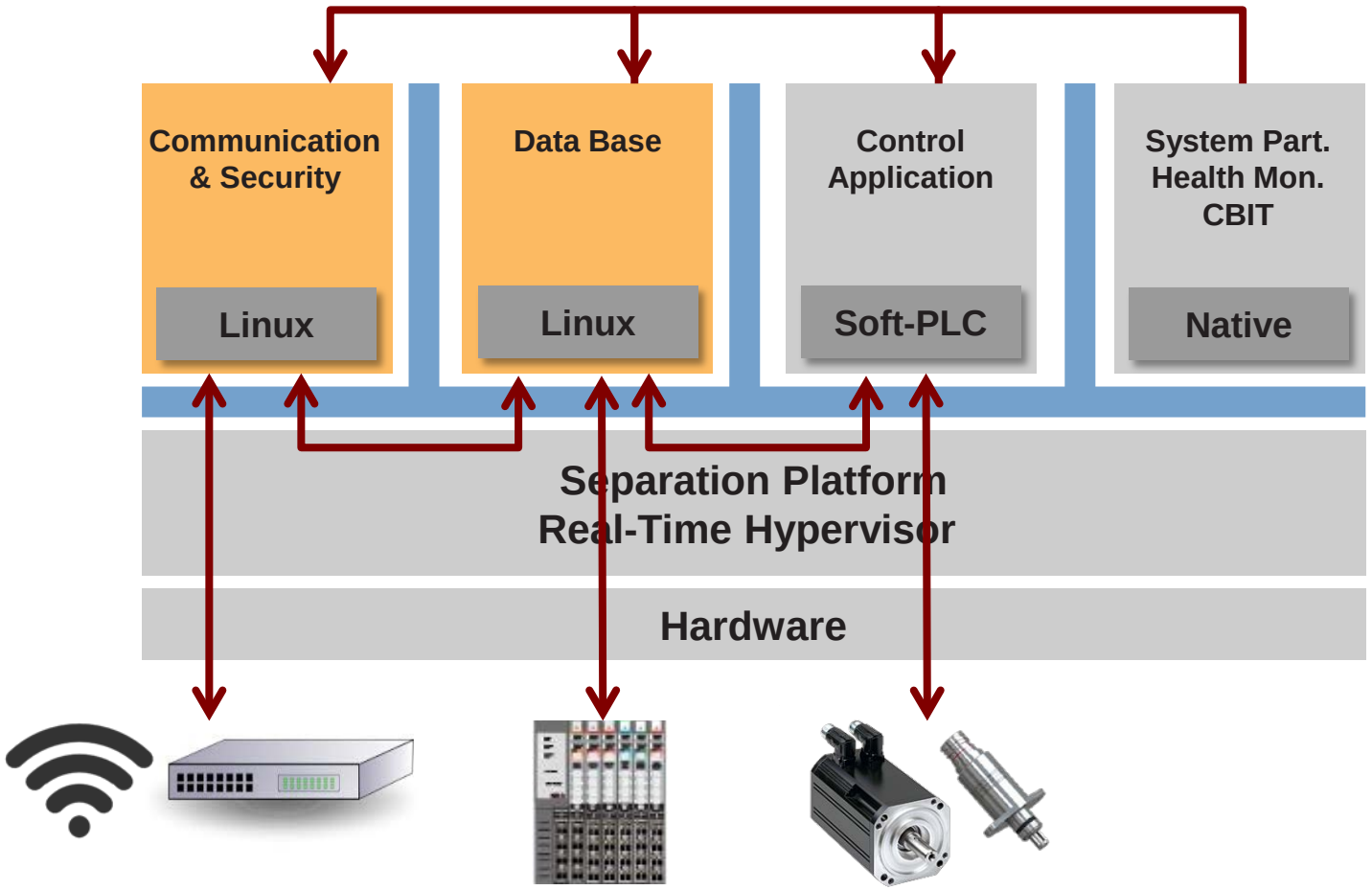
Authentication

Cryptography

Monitoring
Intrusion detection
Perimeter Protection



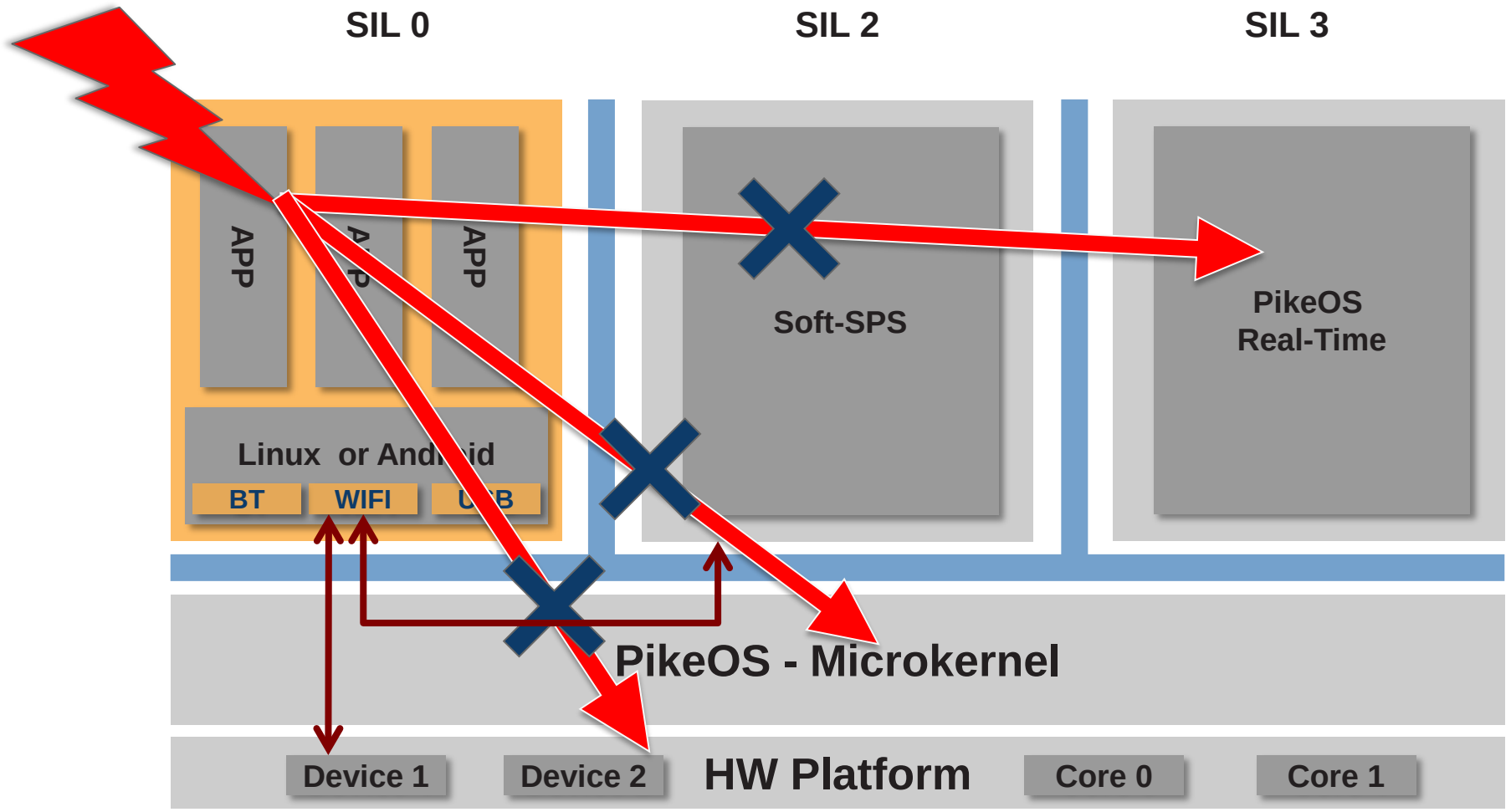
Security by Separation



- MILS: Safety and Security
- HW Obsolescence
- GPL Isolation

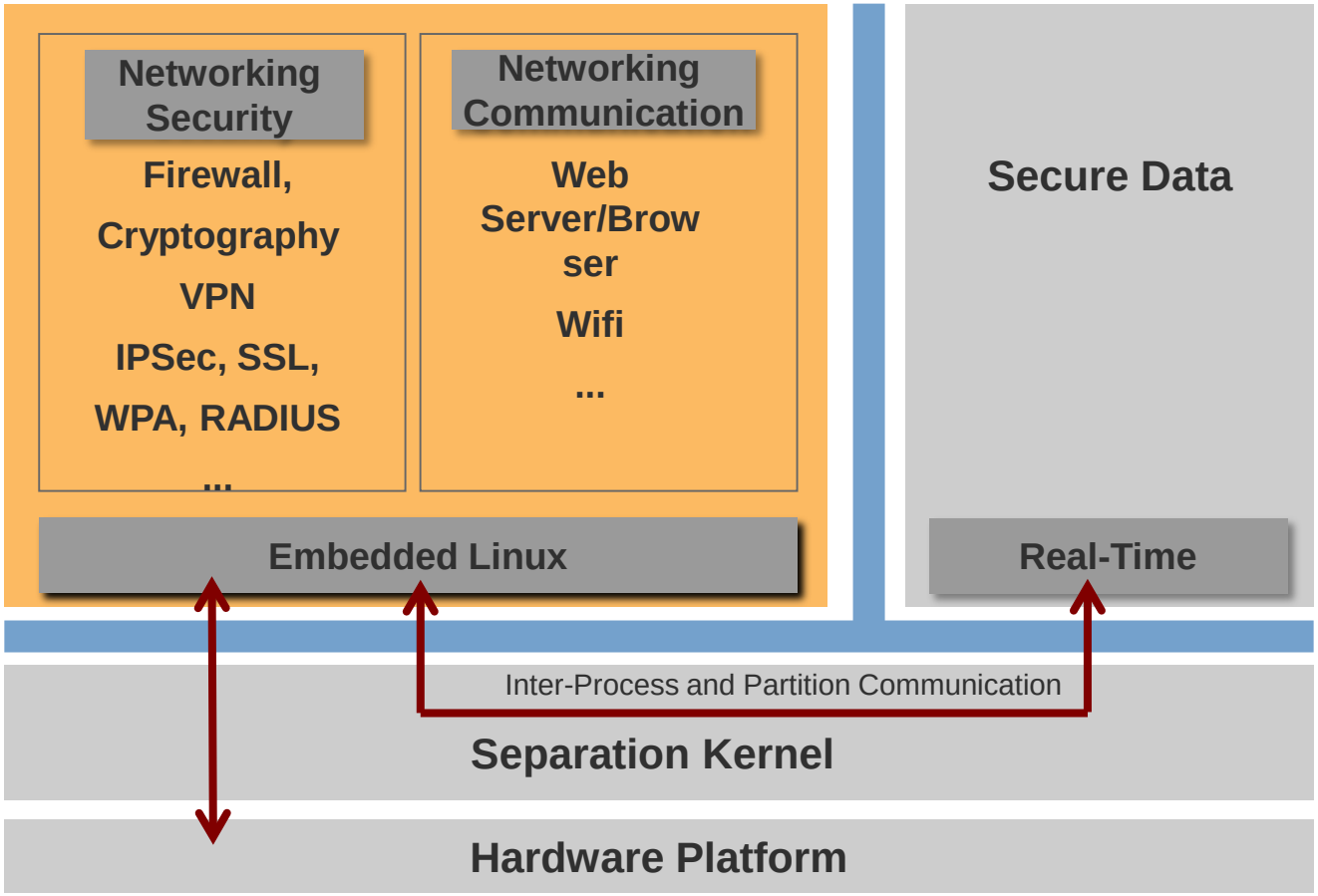
Security by **separation** and **controlled information flow**

Attack Scenario - SW Level



Linux Security

- Network Security ensured by Linux
- Security Updates for Linux

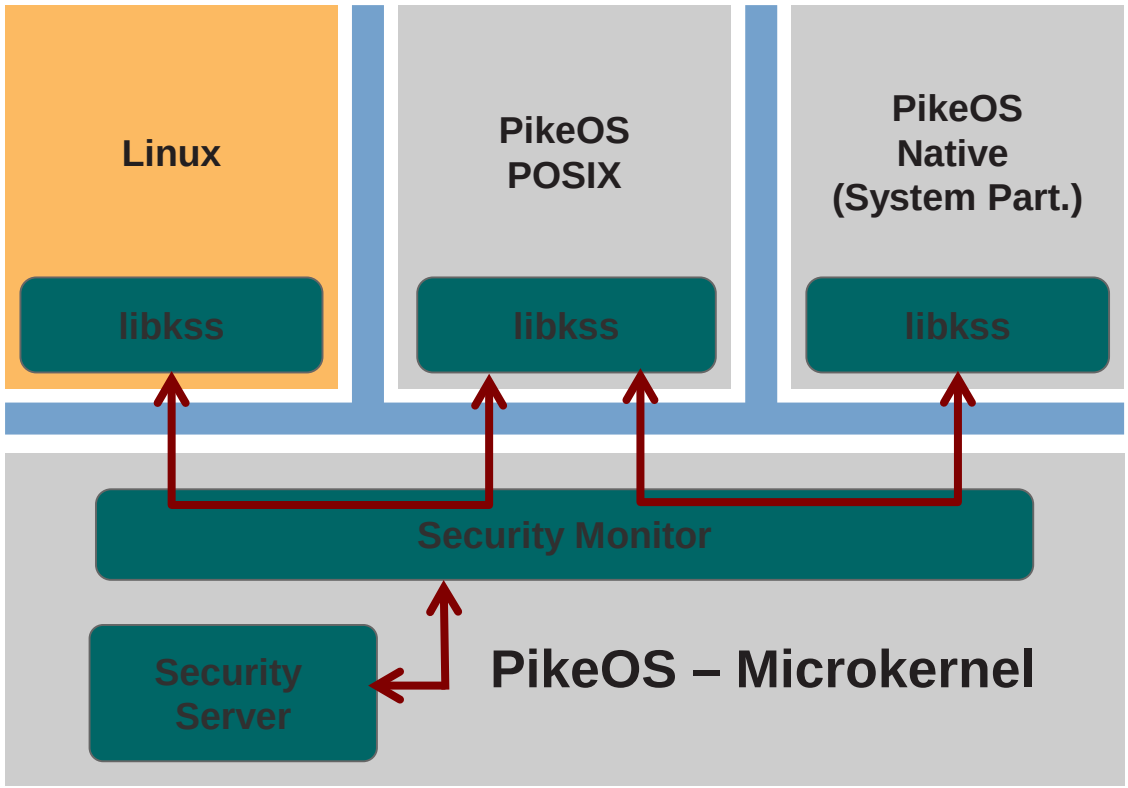


Secure Boot

- **Attack Scenario**
  - Hacking User or Kernel is complicated by Antivirus-SW
  - Replace **boot-loader, boot-image**, Application image…
- **What am I trying to protect?**
  - Against **unauthorized modification** of Firmware and OS image
  - My system from **reverse engineering**/cloning
- **How Do I Protect my System**
  - My SoC provides a **Mode to execute Secure-Boot-Code**
  - **Validate** every instance of **Software loaded on my System**
  - **Root of Trust** to Validate in **Chain of Trust**

PikeOS Use-Case - Security Policy Manager

- **Kaspersky Security System for PikeOS**
- **Application independent from security means**
  - Separate Functionality and Security
  - No limitation by application means
  - Update Application and Security means in dependently
  - System wide security
- **Security Monitor evaluates …**
  - Application behavior
  - System state
- **… and Enforces Security Policy**
- **Security Server**
  - Security Configuration
  - Security Context
  - Takes Access Decision

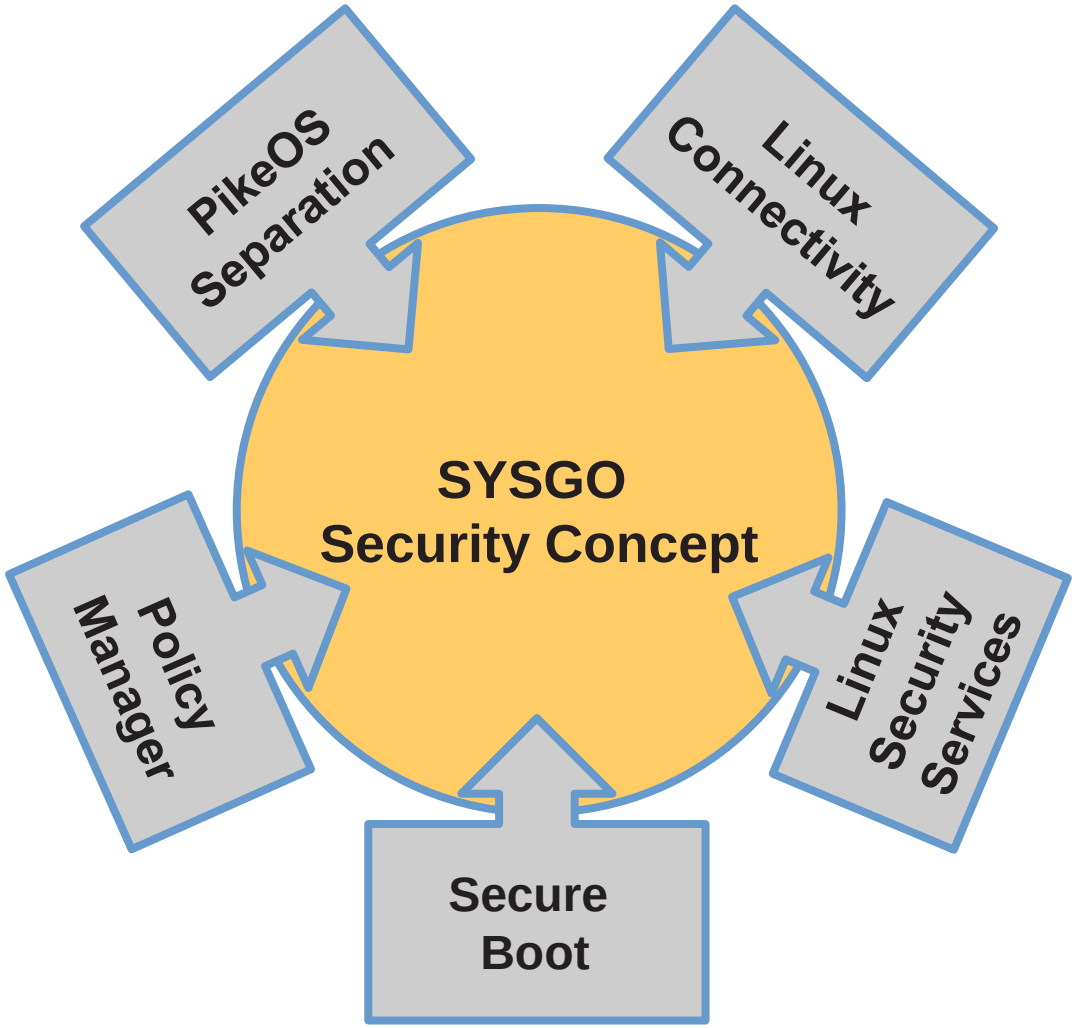


PikeOS - Security Certification

- **CSPN – evaluation criteria of French Authority**
  - French Information Security Agency (ANSSI)
    - Certification de Sécurité de Premier Niveau" (CSPN)
  - Comparable to Common Criteria EAL4+

- **Common Criteria and IEC 15408**
  - PikeOS Security Target
    - based on EURO-MILS PP
  - Targeting EAL5+/EAL6
  - Ongoing Certification at BSI: BSI-DSZ-CC-0923

SYSGO IoT Security Solution - Summary




SYSGO
EMBEDDING INNOVATIONS
Thank you for your attention!
More information on www.sysgo.com