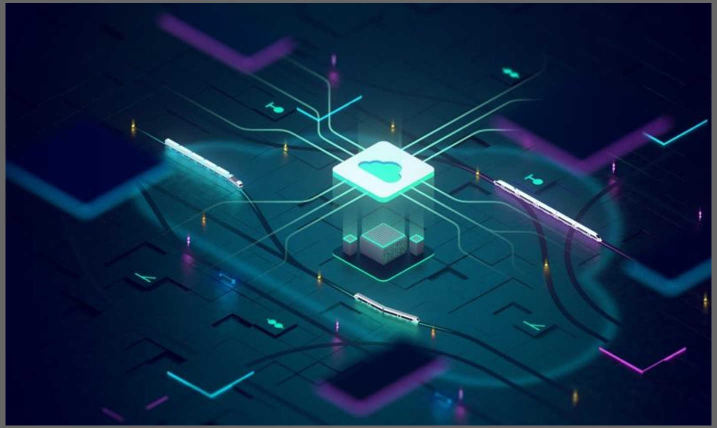
Interlocking in the Cloud

Sonja Steffens, Siemens Mobility GmbH



AUSTRIA VIENNA 2024
IRSC INTERNATIONAL Railway Safety Council

17-21 Sept. 2024

Vienna, Austria
Aula der Wissenschaften

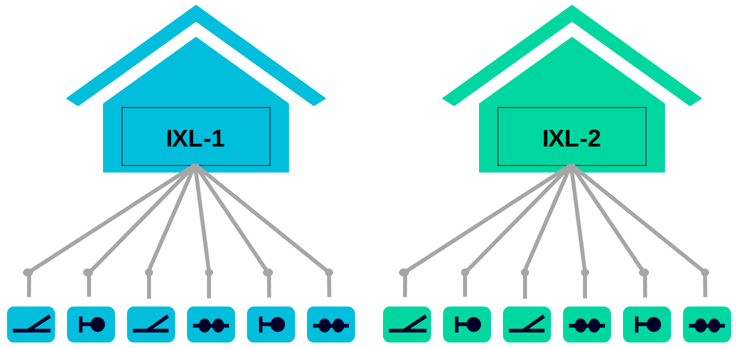
Architectural Evolution in Railway Signaling

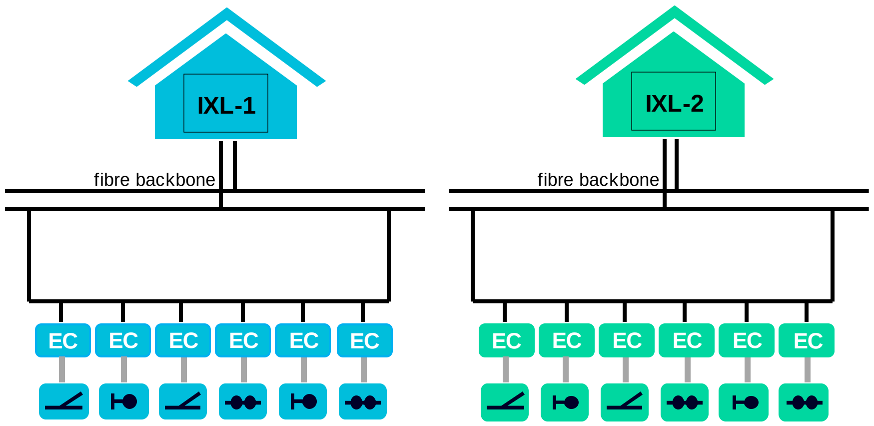
Electronic Interlocking

- Proprietary architecture
- Radical copper cabling
- Limited control distance
- Decentralized logic

Digital Interlocking "DSTW"

- IP based architecture
- Standardized communication (e.g. EULYNX)
- Unlimited control distance
- Centralization possible
- IT security



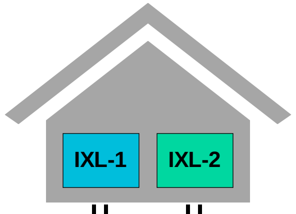


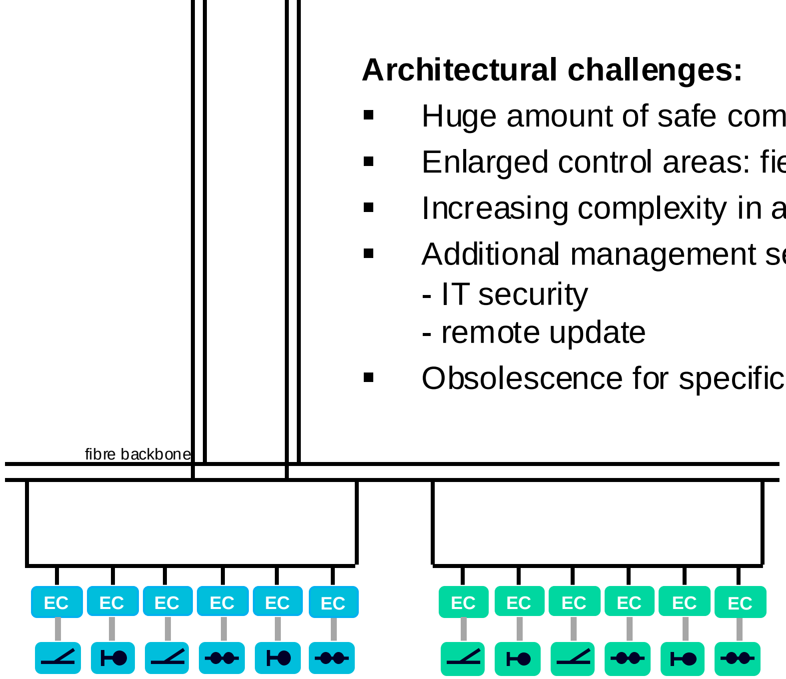
IXL: Interlocking | EC: Element Controller

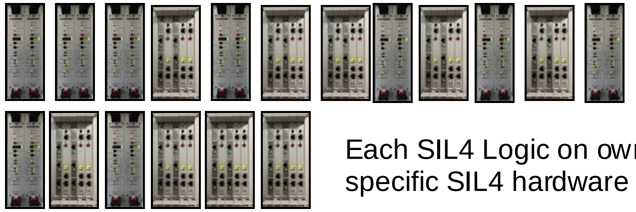
AUSTRIA VIENNA 2024 IRSC INTERNATIONAL Railway Safety Council

Centralized Rail Data Center

2024:







Each SIL4 Logic on own specific SIL4 hardware

Architectural challenges:

- Huge amount of safe comm. connections
- Enlarged control areas: field elements, trains
- Increasing complexity in applications
- Additional management services:
  - IT security
  - remote update
- Obsolescence for specific SIL4 hardware !

Future: 2013-15 Research Project

aramis AUTOMOTIVE · RAILWAY · AVIONICS MULTICORE SYSTEMS KIT

Multicore Standard Technology
„commercial-off-the-shelf“ (COTS)

Challenges:

- SIL4 applications (safety & availability)
- COTS multicore technology
- HW independency
- Mixed SIL
- EULYNX conformity
- Migration of existing applications as interlocking logic, radio block center, …

Distributed Smart Safe System
DS3

IXL: Interlocking | RBC: Radio Block Center | ATO: Automated Train Operation | SIL4: Safety Integrity Level 4 | COTS: commercial-off-the-shelf

Distributed Smart Safe System (DS3) – Safety Principle

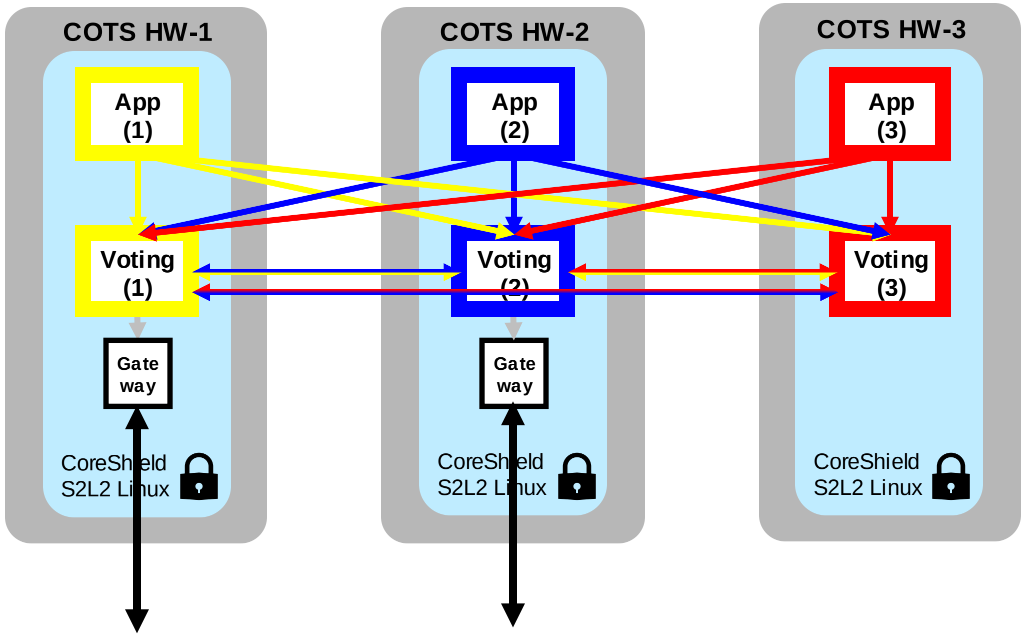
diversity & redundancy & voting ▶ safety

additional redundancy ▶ availability

- Each **safety critical** software is running in at least two parallel instances (1/2) with diverse = **colored** safety mechanism on separate CPUs.
- The results of the **App** instances are compared by a safe **Voting**
- Results of the voting are sent out to other systems via protocol **Gateway**
- For increased **availability** a 3rd instance is used to achieve "2-out-of-3"
- As operating system and IT security layer the CoreShield S2L2 Linux is used.

2-out-of-2 for safety

2-out-of-3 for availability



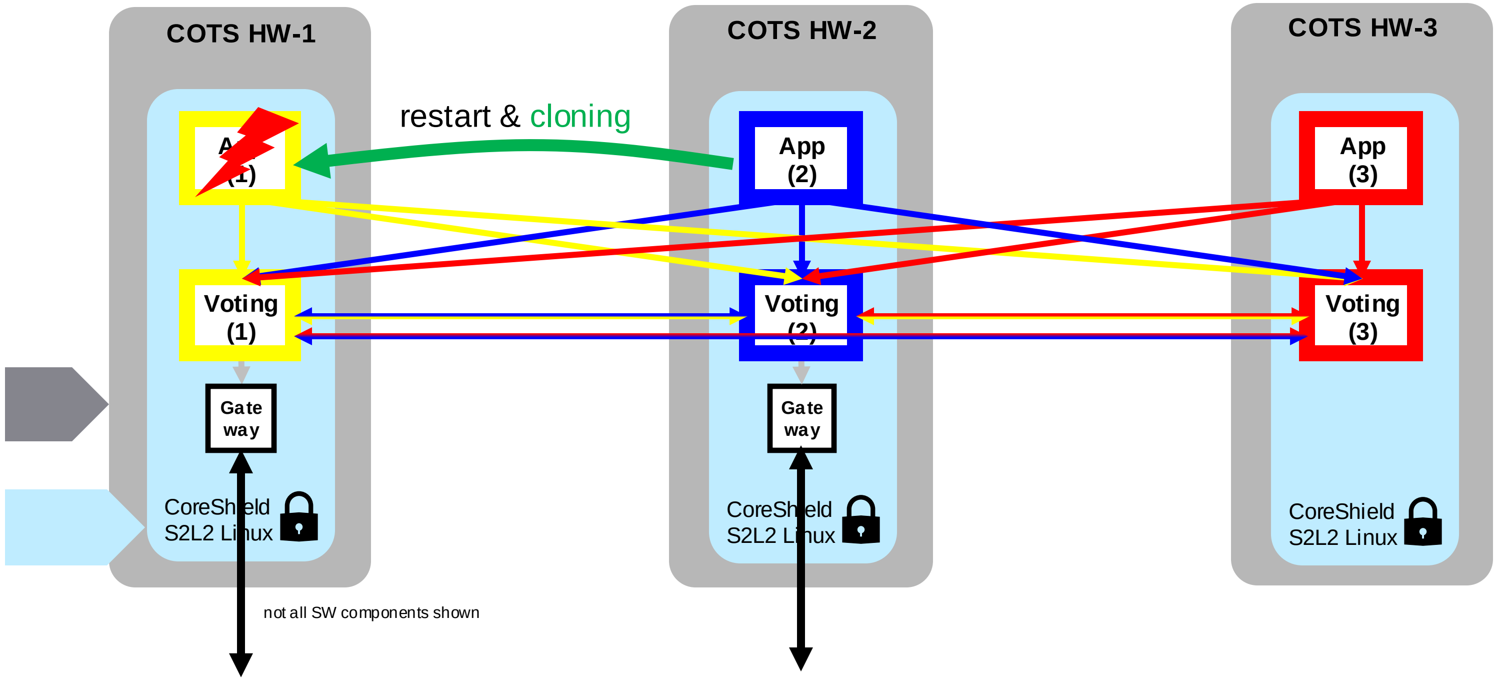
Colored = diverse scattered memory management is instrumented into the safety critical source code to ensure that any common cause failure within the non-safety-critical parts (COTS HW, HW abstraction layer, operating system) or any influence by other software is identified in a safe way.

Availability and Maintenance

SW restart
during runtime

HW replacement
during runtime

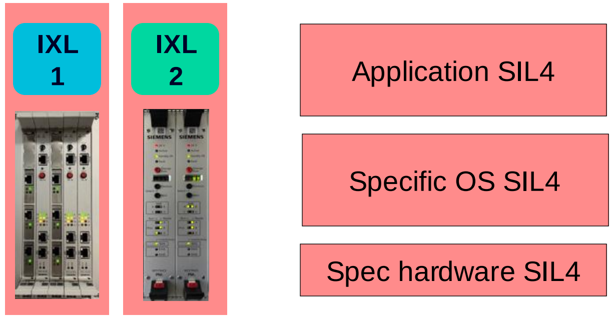
IT-security patches
during runtime



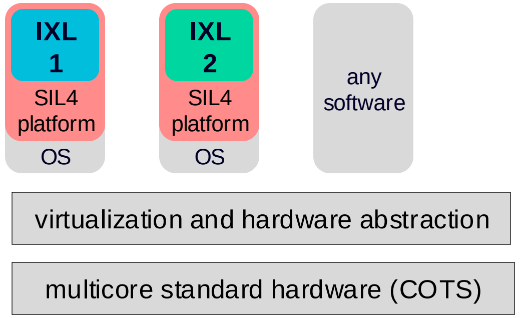
- DS3 provides efficient maintenance of COTS hardware or IT security patching during runtime
- DS3 supports geographical redundancy by distribution of the software on different locations

Innovative Signaling Architecture - Benefits

Traditional Signaling Architecture



Innovative Signaling Architecture



State of the art:

- specific safety platform (hardware + software)
- Performance not scalable
- Each system on own hardware
- Various variants of specific hardware
- Complicated obsolescence management

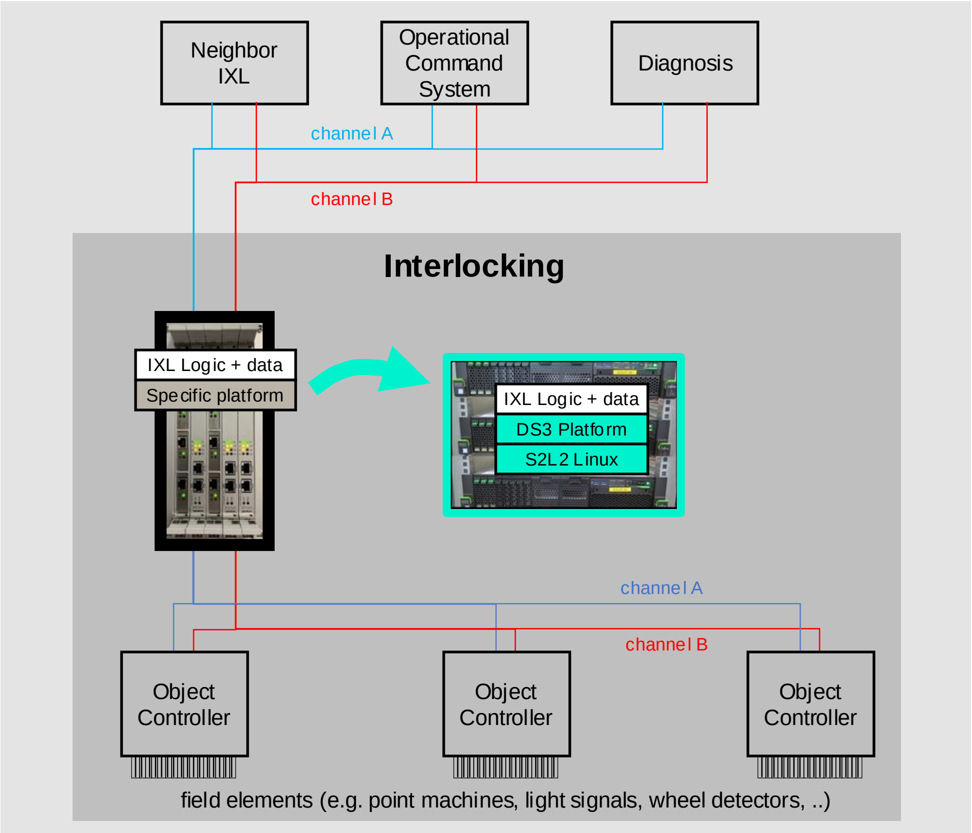
Benefits:

- Usage of **high performant** multicore technology (**COTS**)
- Severals systems on same hardware: **reduction** of needed **hardware, space and energy**.
- Applications with **different SIL** on same hardware possible
- High grade of **automation** for SW maintenance
- Lean **IT-security** patching during runtime (highest availability)
- Common hardware portfolio with **simple obsolescence**
- Distribution of the software to provide **geographical redundancy**

COTS: Commercial off-the-shelf | IXL: Interlocking | OS: Operating System | SIL4: Safety Integrity Level 4

Introduction of DS3: Pilot Project Interlocking in Austria

DS3 Pilot Project:
Interlocking Trackguard Simis AT



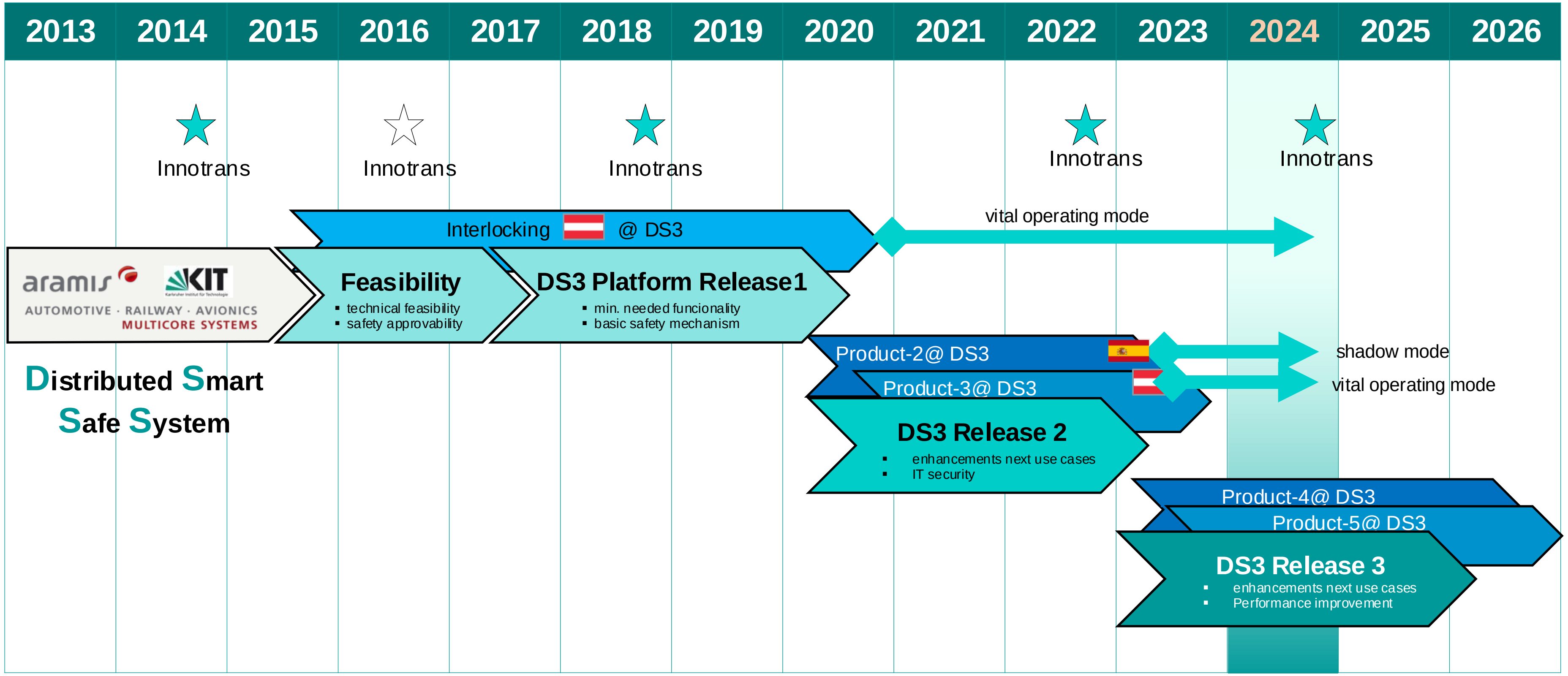
Product migration to DS3:

- Approved customer IXL logic untouched, identical application SW and data
- Interfaces to connected systems untouched
- COTS HW type identical to proven COTS HW used by operational command systems

Result after 4 years: **100% availability !**

COTS: Commercial off-the-shelf | IXL: Interlocking | S2L2 = Siemens Secure LongLife

DS3 – from Research Project to Customer Project and stepwise ongoing ..



Thank you for your attention!