ONE Linux Distro to rule them all

How to unify Linux usage accross your organization

SIEMENS

Benjamin Schilling

Siemens Mobility GmbH
Braunschweig

Product Lifecycle Manager
– Secure Operating Systems
Senior Key Expert
– Platform Security

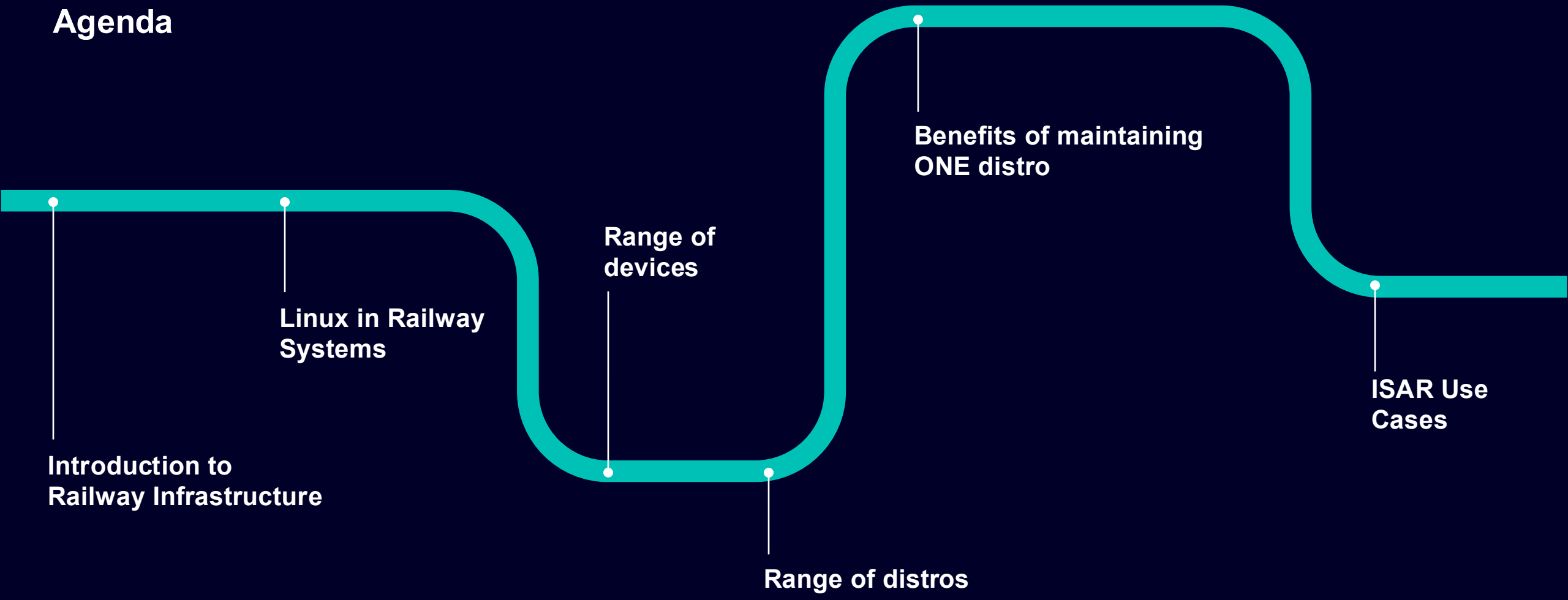
Work Experience with ISAR
- Working with ISAR since 2017
- We built a platform used in many products based on ISAR

Ask me anything on
- Operating System Security
- Secure System & Product Architecture
- Hardware Security Solutions

Hottest (non ISAR) OSS topics right now:
- EU CRA and challenges for OSS
- Zephyr RTOS

SIEMENS

Agenda



SIEMENS

Railway Infrastructure Purpose & Terminology

- Purpose
  - Ensure RAMS of train traffic
    - Reliability – Correct train arrives at specific point in time
    - Availability – Trains can run 24/7
    - Maintainability – Redundancy allows maintenance without interruption of traffic
    - Safety – Train collisions/derailments are avoided

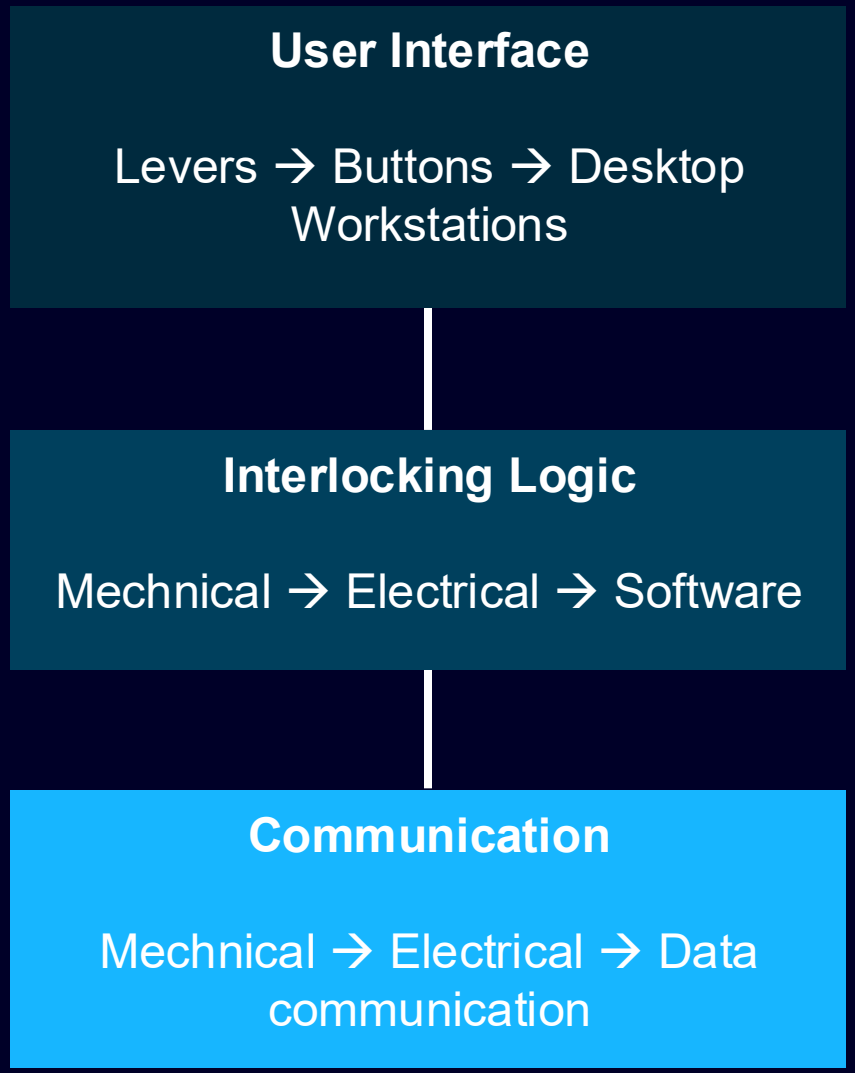
- Field elements → Components placed besides the track that fulfill rail automation purposes
  - Points → Allow changing tracks
  - Axle Counters → Are placed at start and end of track area split one pair of rails in many sections
  - Signals → Provide e.g. speed indication for train driver
- Interlocking → Safety logic preventing collisions of trains on tracks
- Automatic Train Supervision (ATS) → Takes care of dispatching of trains

Three levels of equipment

Operation Control Center

Interlocking

Wayside Equipment

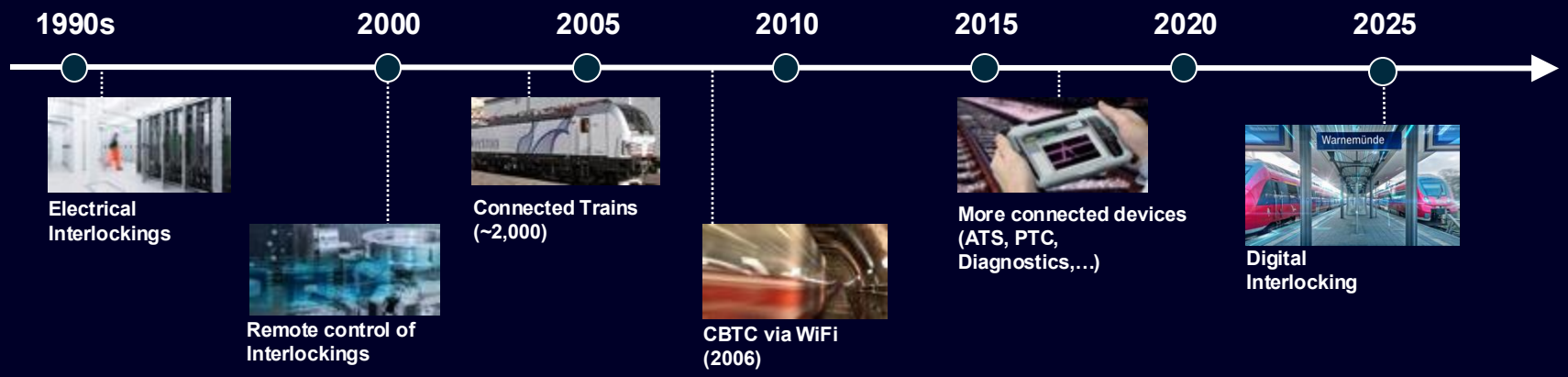


SIEMENS

Challenges – Digitalization/Connectivity

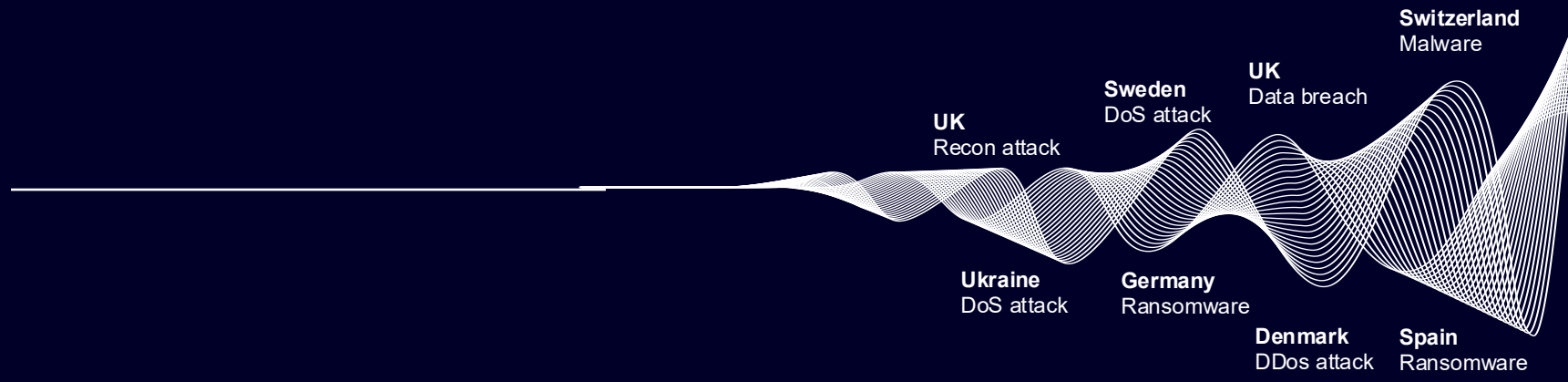
Trends

- More and more software in use
- Increasing connectivity of devices (IoT)
- Communication via public networks



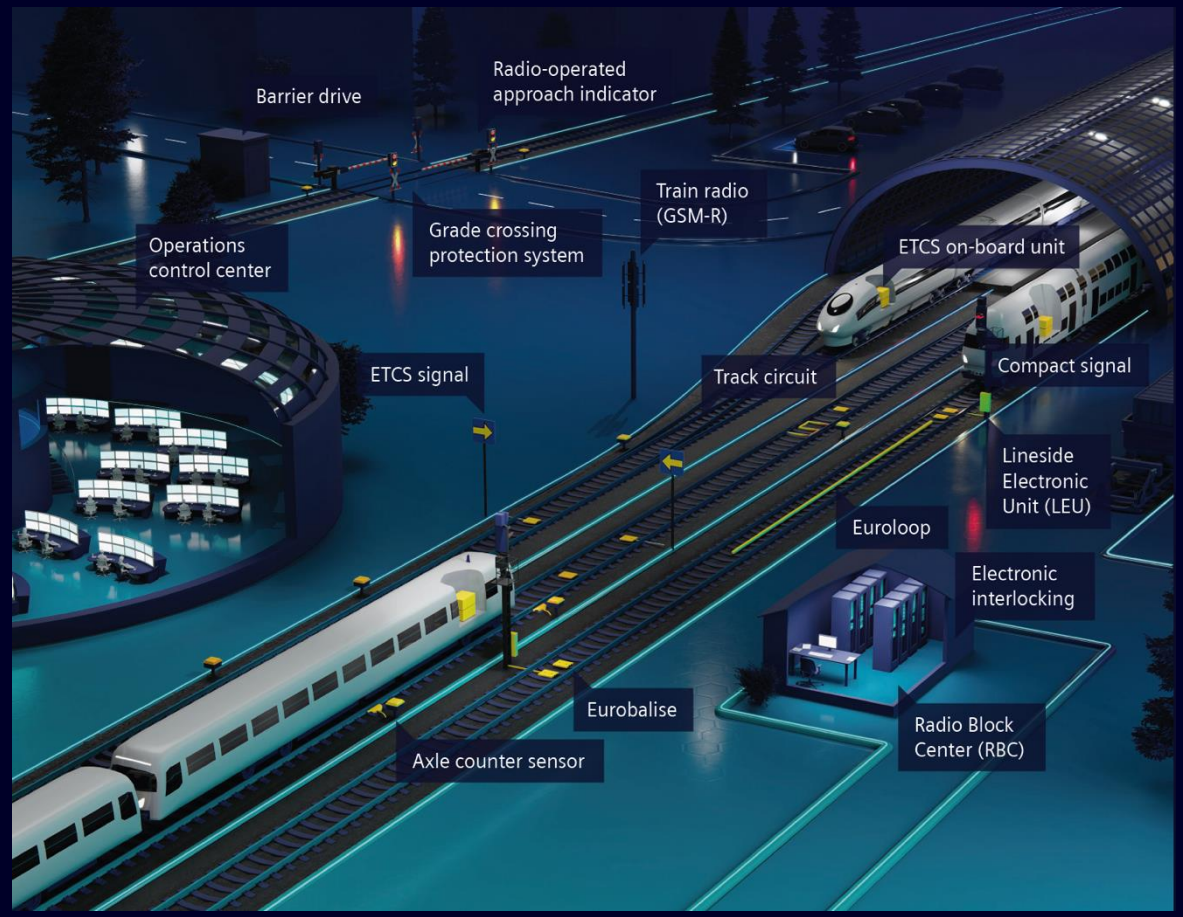
Risks

Number of **cyber attacks** increases and threatens the stability of digital systems

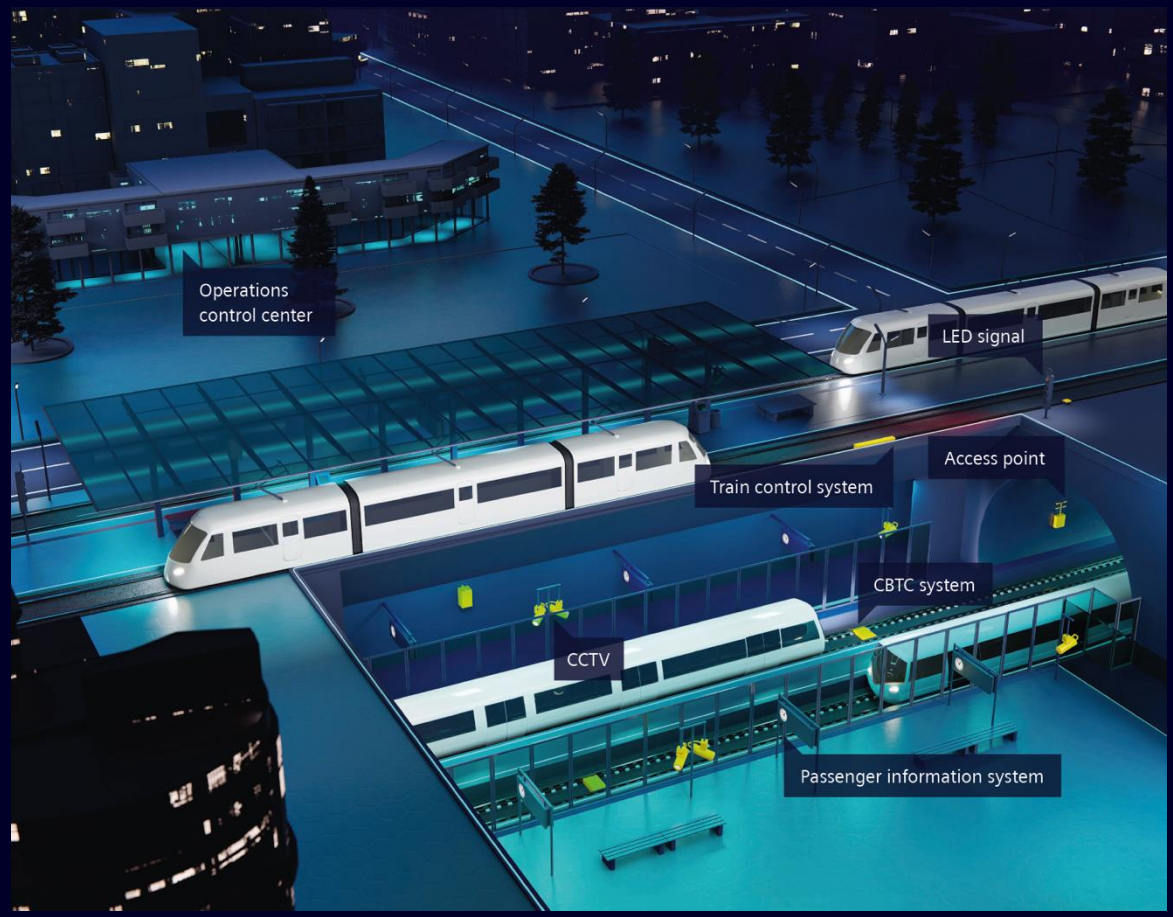


SIEMENS

Railway Systems



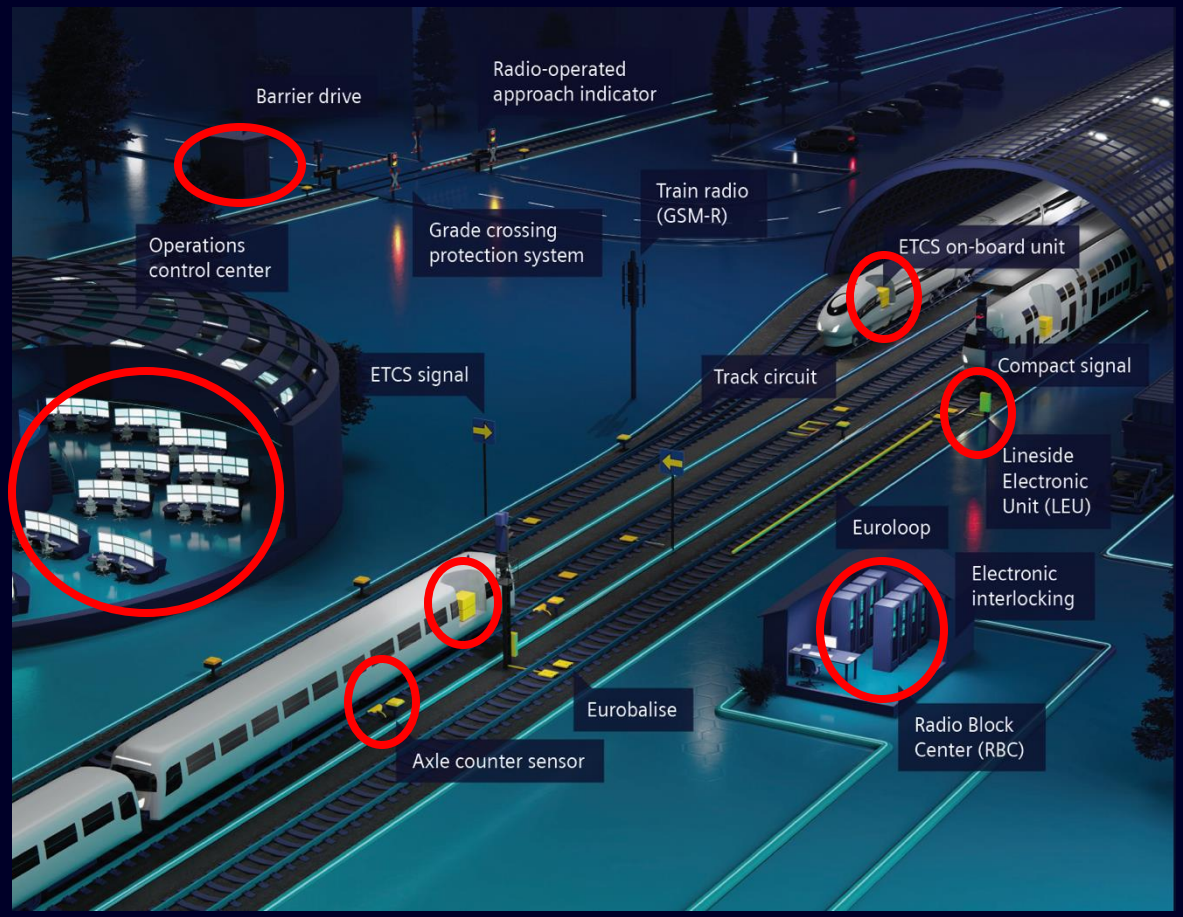
Mainline



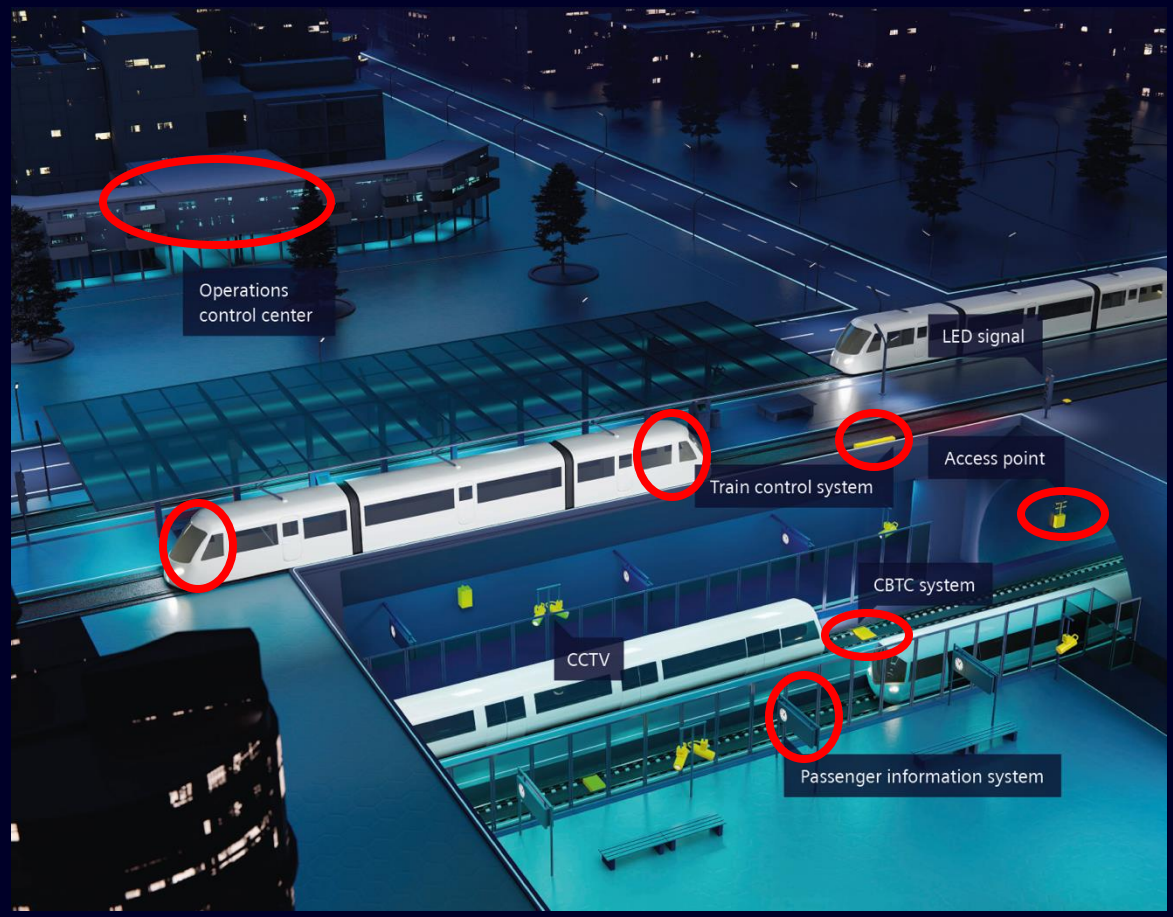
Mass Transit

SIEMENS

Linux in Railway Systems



Mainline

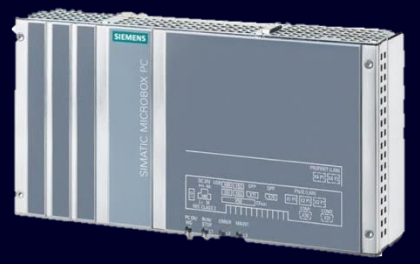


Mass Transit

SIEMENS

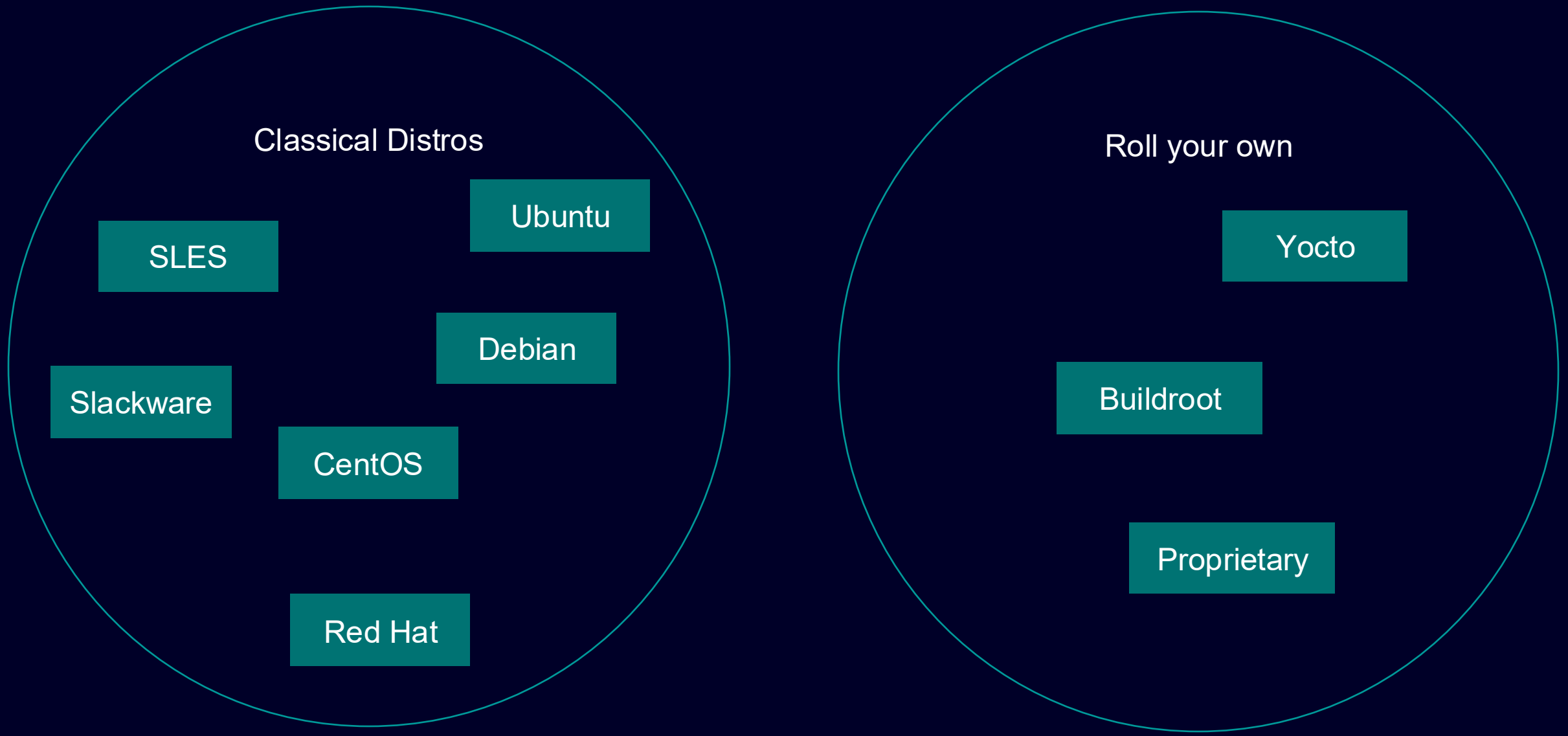
Range of Linux Installations at Siemens Mobility

- **Headless & GUI applications**
- **Embedded to Server** Devices
  - from 4 cores, 400Mhz
  - to >32 Cores, xGHz
- Various **CPU architectures**
  - armhf
  - arm64
  - amd64
- Broad range of connectivity from ethernet to railway specific protocols
- **Installed from control centers to trackside cabinets or mobile devices**



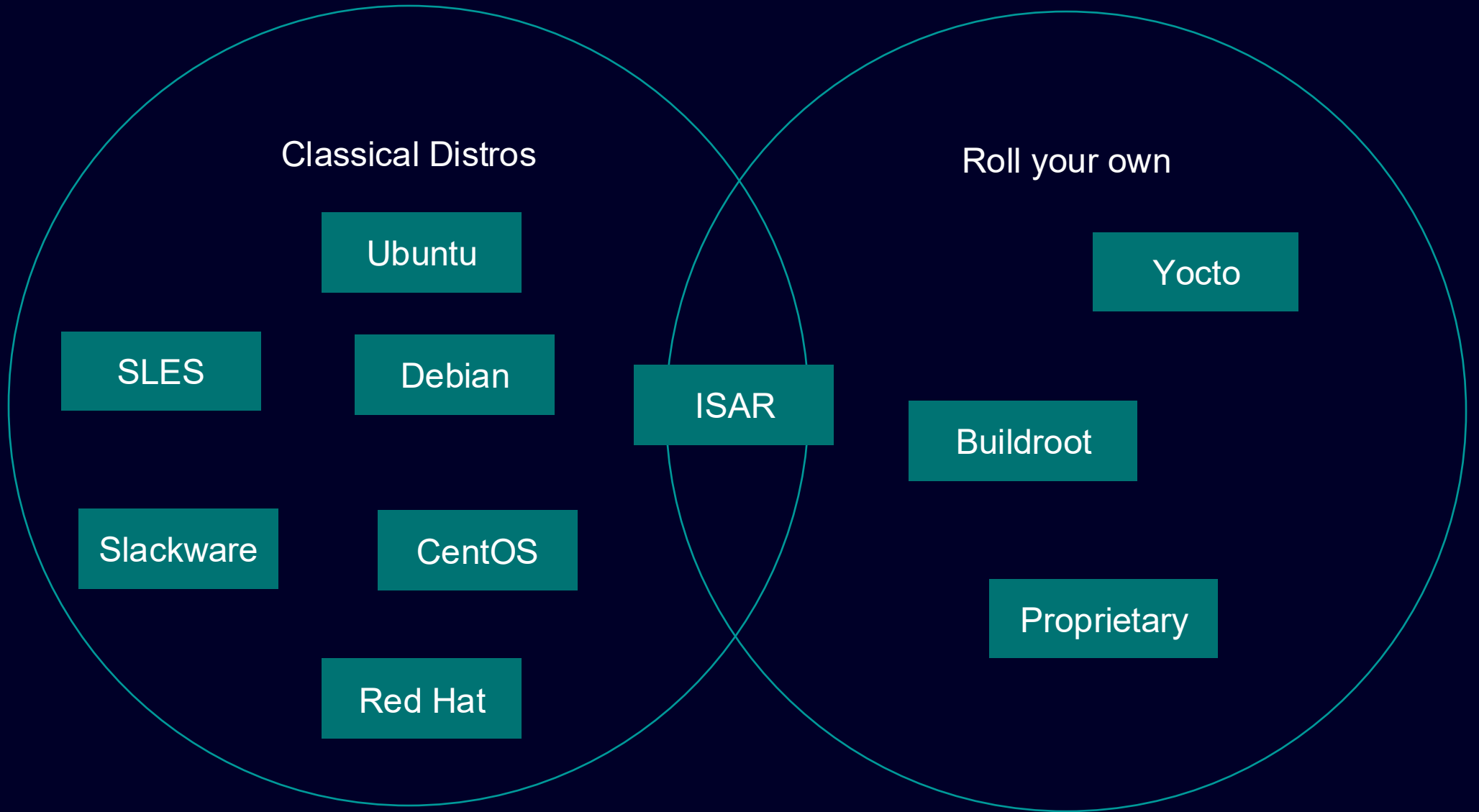
SIEMENS

Range of Linux Distros in use



SIEMENS

Range of Linux Distros in use



SIEMENS

Benefits of maintaining ONE distro based on ISAR and Debian

„Product Software“

- isar-cip-core already provides many blueprints
  - UEFI Secure Boot
  - Rootfs protection via dm_verity
  - A/B Software Update
  - Rootfs encryption
  - …

Build Automation

- Testing
- SBOM Generation
- Software Compliance
- Secure Boot Signing
- …

Cybersecurity

- Reduction of dependency variants
- Hardening
- Vulnerability management
- …

Know-How Sharing

SIEMENS

Use Cases: Solution Engineering

- Typically one-shot engineering projects
- Time to market and price sensitive solutions
- Automation is key

- Legacy
  - Debian (or other distro) installation via USB/DVD
  - Manual or scripted installation of required software
  - Hardening of the resulting installation

With ISAR

- Package definition in recipes
- Easily extensible also for non-Linux-native engineers
- Fosters scripted workflows
- Hardening only for necessary packages
- Flexibility for custom solutions

Use Cases: Product Development
Developing stand-alone devices

Legacy

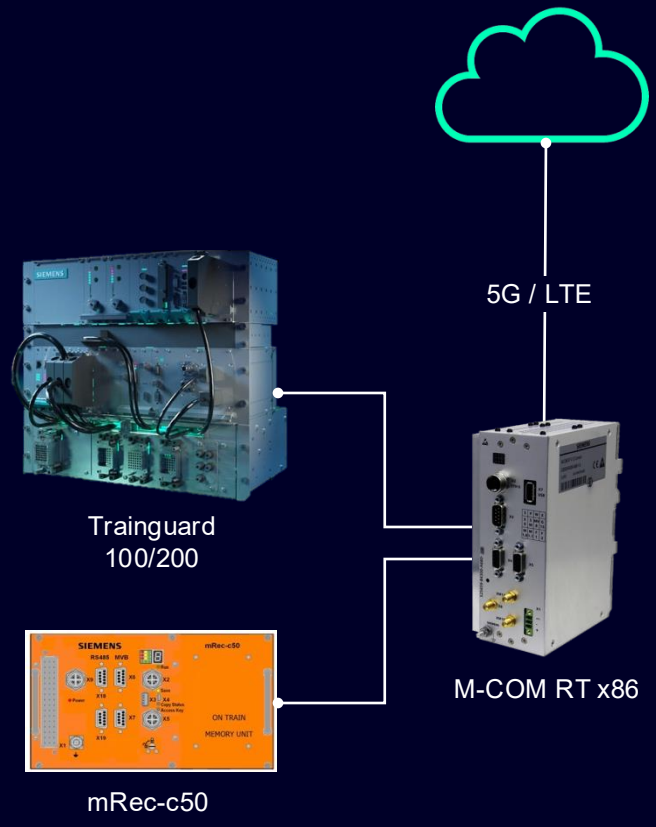
- Teams maintained their own solutions
- Migration to newer distro versions creates issues
- System startup not harmonized
- Build on developer machines
- Software not packaged
- From init scripts to custom init systems

With ISAR

- Build with CI/CD
- Software build as Debian packages
- Easier sharing between products
- System startup via systemd
- Pre-integrated system software (secure boot, swupdate, …)

Upstream BSP in isar-cip-core: Siemens Mobility M-COM RT x86

- Quad Core: Intel E3950 Atom (1,6 GHz)
- Ethernet, MVB, CAN, USB, Serial
- GPS, Wi-Fi, LTE/5G
- Storage: up to 4x 1 Terabyte
- 24-110V wide range power supply
- 35mm standard DIN rail or wall mounting



Certificate No: S113082801 Page 1 / 3

BUREAU VERITAS

Verification of Conformity

Applicant:	**Civil Infrastructure Platform (CIP)**
Certificate Coverage (including Version):	**CIP product security development lifecycle & process V1.0**
Standard(s) used:	**ISA/ IEC 62443-4-1:2018**

We, **Bureau Veritas Consumer Products Services (H.K.) Ltd., Taoyuan Branch**, declare that the process above has been verified and found compliance with the requirement limits of applicable standards. The test record, data evaluation and process represented herein are true and accurate under the standards herein specified.

Requirements Assessed:

Security management (12,1,13)
Specification of security requirements (5,0,5)
Secure by design (2,2,4)
Secure implementation (0,2,2)
Security verification and validation testing (4,1,5)
Management of security-related issues (6,0,6)
Security update management (5,0,5)
Security guidelines (4,3,7)

ShangJyh Lin

ShangJyh Lin / Expert
Aug. 28, 2024

BUREAU VERITAS Consumer Products Services

SIEMENS

Use Cases: Platform Development
Centralization of commonly needed functionality for products

Legacy

- Different build systems accross plattforms
- From yocto, buildroot to proprietary
- Product developers need to understand how to build products with this platform

With ISAR

- Commonly used parts available as layers
  - Internally used software
  - Build different types of images (raw, oci, vm)
  - Centralized Debian Mirrors
  - Automation for 3rd Party Software Compliance
  - Know-how for only one build system needed

Questions?

SIEMENS

Disclaimer

Subject to changes and errors. The information given in this document only contains general descriptions and/or performance features which may not always specifically reflect those described, or which may undergo modification in the course of further development of the products. The requested performance features are binding only when they are expressly agreed upon in the concluded contract.

All product designations may be trademarks or other rights of Siemens AG, its affiliated companies or other companies whose use by third parties for their own purposes could violate the rights of the respective owner.

Contact

Published by Siemens Mobility GmbH

Benjamin Schilling
Product Lifecycle Manager – Secure Operating Systems
Ackerstraße 22
38126 Braunschweig
Germany

E-mail schilling.benjamin@siemens.com

SIEMENS