PHILIPP M. SCHOLL, THANIKESAVAN SIVANTHI, TOBIAS DOERR, NICOLAS COPPIK, MICHELE MARAZZI

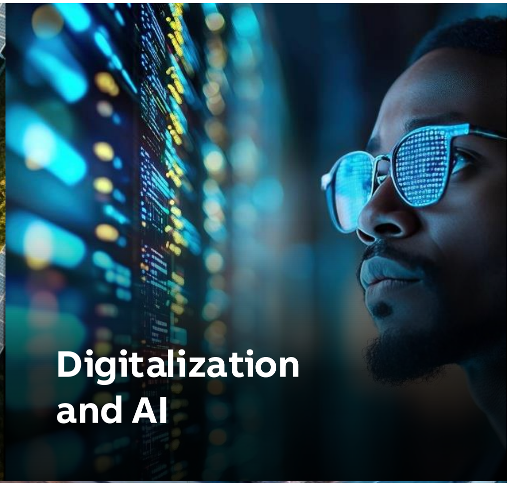
EVOLVING LEGACY SYSTEMS FOR STRONG SPATIAL AND TEMPORAL ISOLATION

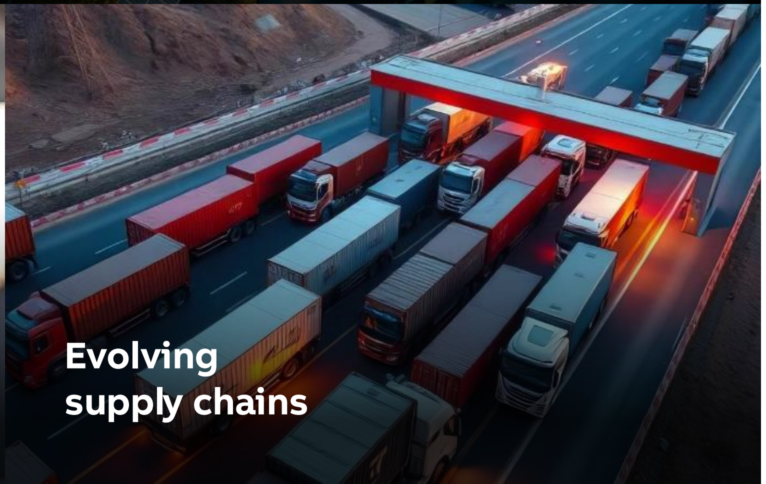
ABB CH.CRC.S2 – Industrial Software Solutions

ENGINEERED TO OUTRUN

ABB purpose and offering align with key global megatrends

Key Global Megatrends





Stand-out value proposition of combined electrification & automation

CUSTOMERS

Business area **Electrification**

Business area **Automation**

Business area **Motion**

~65% electrification

ABB

~35% automation

ABB Corporate Research

~350 highly qualified scientists and engineers

6 corporate research and technology centers around the world

Business aligned research with 7 core technologies

>200 technology projects and pre-studies

>200 FFs and **>200** publications

Västerås
SE

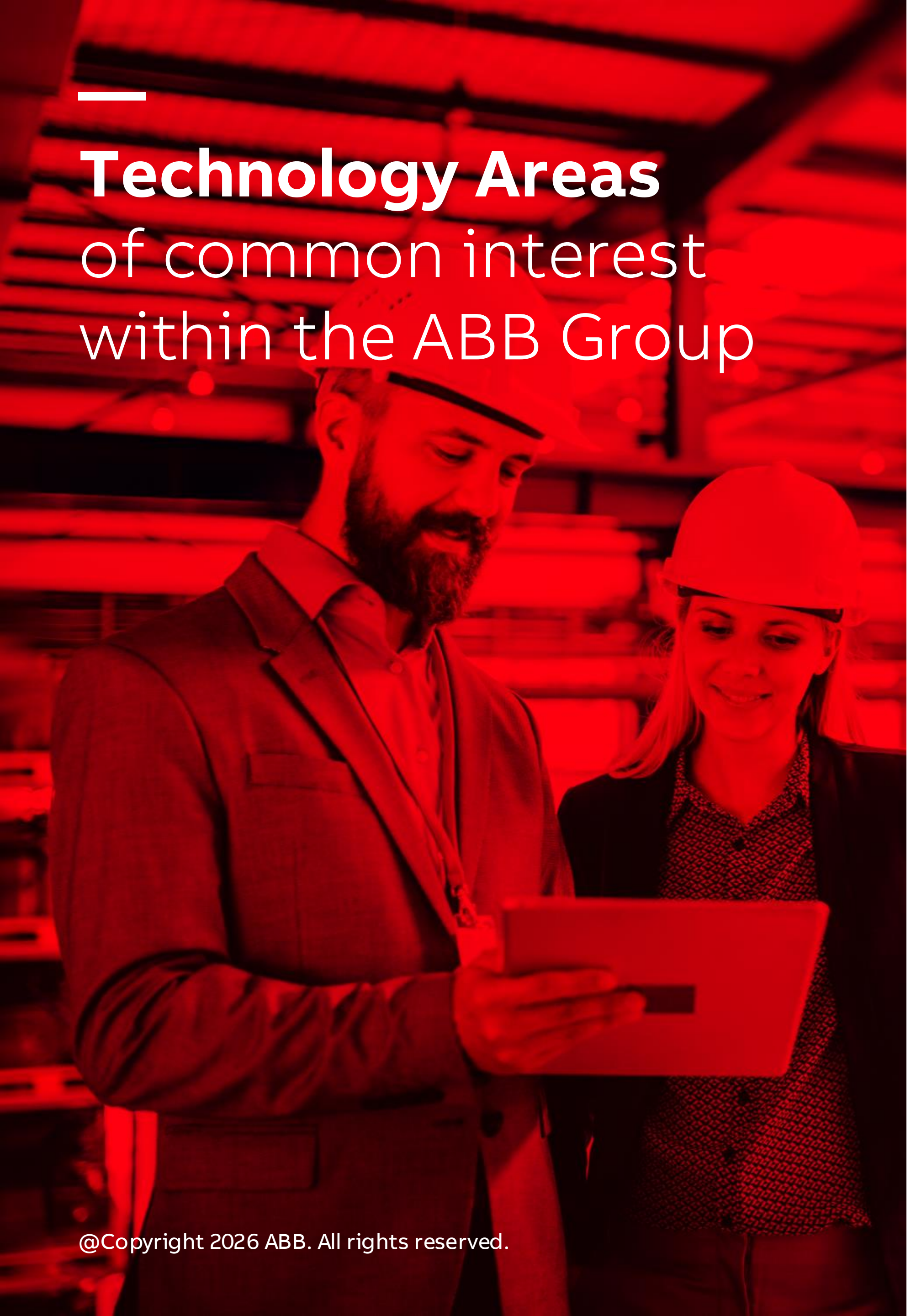
Mannheim
DE

Bangalore
IN

Baden Dättwil
CH

ABB Corporate Research Center Switzerland

Inaugurated in 1973



Technology Areas of common interest within the ABB Group

Multiphysics drive sustainability-oriented innovations in products and solutions. Multiphysics is the study of multiple interacting physical properties, and we improve productivity by merging physical properties with digital transformation

Mechatronics develop intelligent products by integrating mechanical, electrical/electronics, software, control and sensing components into one system

Power Electronics develop technologies for solid state power electronics (PE). PE enables conversion, control and protection of electrical power in applications like industrial drives, robotics, EV chargers, marine, mining, ultra-fast breakers and direct current (DC) distribution

Technology Areas of common interest within the ABB Group

Connected Systems study and implement the technologies, methodologies and architectures necessary to simplify the access and use of systems, as well to enable seamless and standardized access to information

Sensing create solutions to transform real-world parameters into valuable information using competencies ranging from sensing technology and signal processing to information extraction and sensor system design

Switching explore technologies for current interruption, from arc physics and gaseous insulation, to new interruption and breaker actuation principles, and up to the integration and coordination of protection and control devices at system level

Software & Control design efficiently engineered, user-friendly, sustainable software solutions for industrial control, optimization, and autonomy

System Examples

ABB AC800 Power Electronics Platform

- Multi-Core ARM platform with FPGA fabric
- Real-time critical control software specified with Simulink
- Non-critical tasks run (isolated) side-by-side
- e.g. used for power conversion in trains

ABB Smart Substation Control 600

- Multi-Core X86 platform
- Real-time critical control software specified with SCL
- SCL = Substation Control Language (XML, graph-based)
- Non-critical tasks run (isolated) side-by-side
- e.g. used to execute critical grid monitoring/protection

Challenge: EU's Cyberresilience Act

Cyberresilience Act at a Glance

Report Obligation

11. September 2026

- Mandatory reporting of actively exploited vulnerabilities
- via SBOM
- report severe incidents within 24 hours
- established vulnerability handling process

Full Compliance

11. December 2027

- All products with digital elements must comply, CE marking
- Critical products require third-party certification and partitioning OS
- e.g. in Germany, certification packages for commercial partitioning operating systems: pikeOS, SUSE Enterprise Linux, L4RE…

CRA Established

…

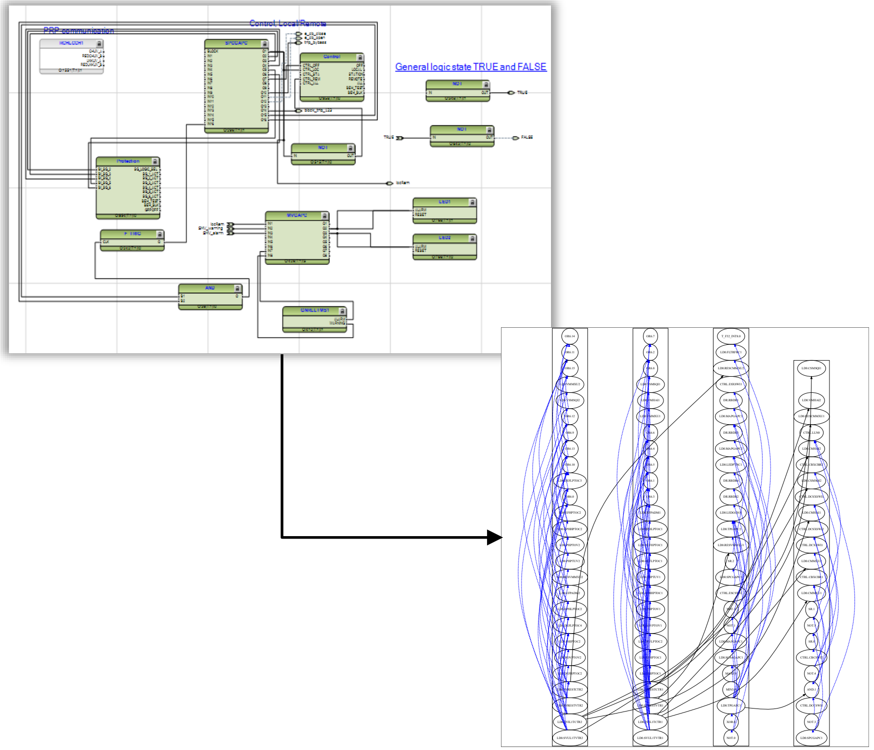
- vulnerability and incident monitoring
- software design has direct influence on cost of testing and re-certification
- “Minimize attack surfaces” as much as possible

drive towards cost reduction for testing and re-certification

Compile-Time Protection and Control

Substation Control Language to seL4/microkit .system

SCL -> seL4.system



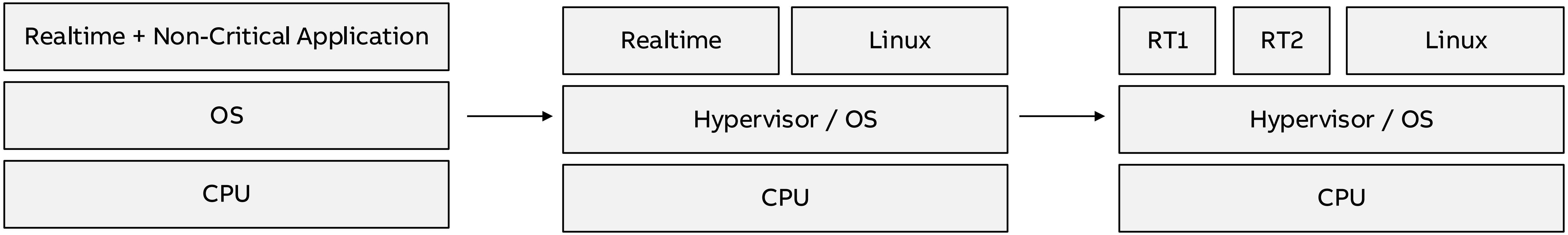
Five Steps

1. benchmark individually with LinuxVM/stress-ng to extract WOET of each block
2. extract graph from SCL with topological order
3. MILP solve for “optimal” CPU/Cache distribution and collapsing chain calls (also to work around 62 PD limit)
4. translate remaining blocks into protection domains (PD)
5. execute…

- periodic activation via timer from root node
- monitoring via mixed-criticality scheduler
- report CPU load, i.e. completion time for application

- Why? minimal scheduling and data exchange overhead, and early error detection

Concurrent Monotholic to Partitioned, Single-Thread



From Monotholic, Multi-Threads to Partitioned, Single-Thread

How to?

Identifying Concurrency Primitives

- find out how threads are synchronized (e.g. semaphores)
- map them to microkit/seL4 primitives

- can often be spotted by particular code patterns
- code analysis and tracing

- transfer to .system description gathers a nice view of the concurrency/activation patterns.

Identifying Shared Memory

- find global symbols that are accessed by now separated tasks
- map them to shared memory

- sometimes separated in c code already
- tracing with qemu, and finding intersecting memory access

- microkit modification:
  - paint required symbols to ".shared" section
  - link into additional "shrd" memory segment
  - map frames in "shrd" for cloned .elf files onto first clone

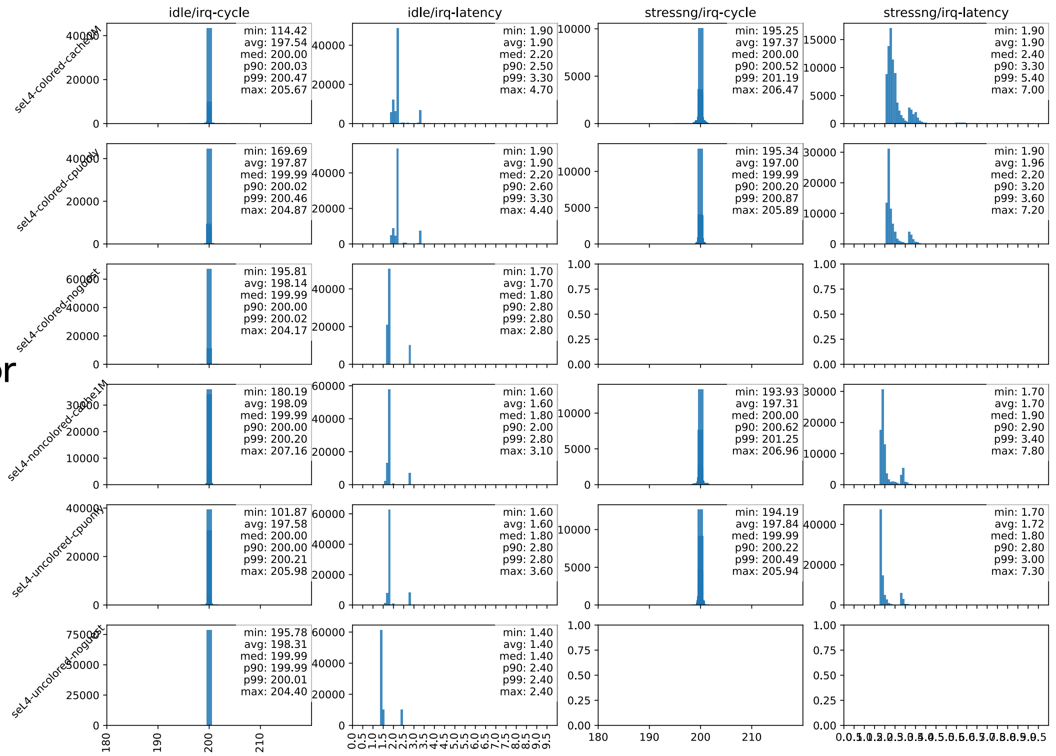
Tracing with qemu's is your friend.

Microkit/seL4 Experiments
Cache-Coloring

- why?
  minimize cross-PD influence when cache-partitioning hardware is absent

- how?
  - -fdata-sections and –ffunction-sections for seL4 kernel
  - distribute to cache line 0 with linker script modification
  - microkit: allocate protection domain's frames according to cache-color
  - missing: allocation of CSpace objects
  - alternative: modify capdl-initializer

- but?
  - no measurable effect as of yet



Conclusion

- Experiments with microkit/seL4 on ABB's protection and control software

- Microkit/seL4 shows great potential to prepare for challenges from
  - Cyberresilience Act for stronger isolation of components
  - Testing effort optimization by stronger isolation of components

- Adoption Hurdles stem mainly from different software designs

ABB