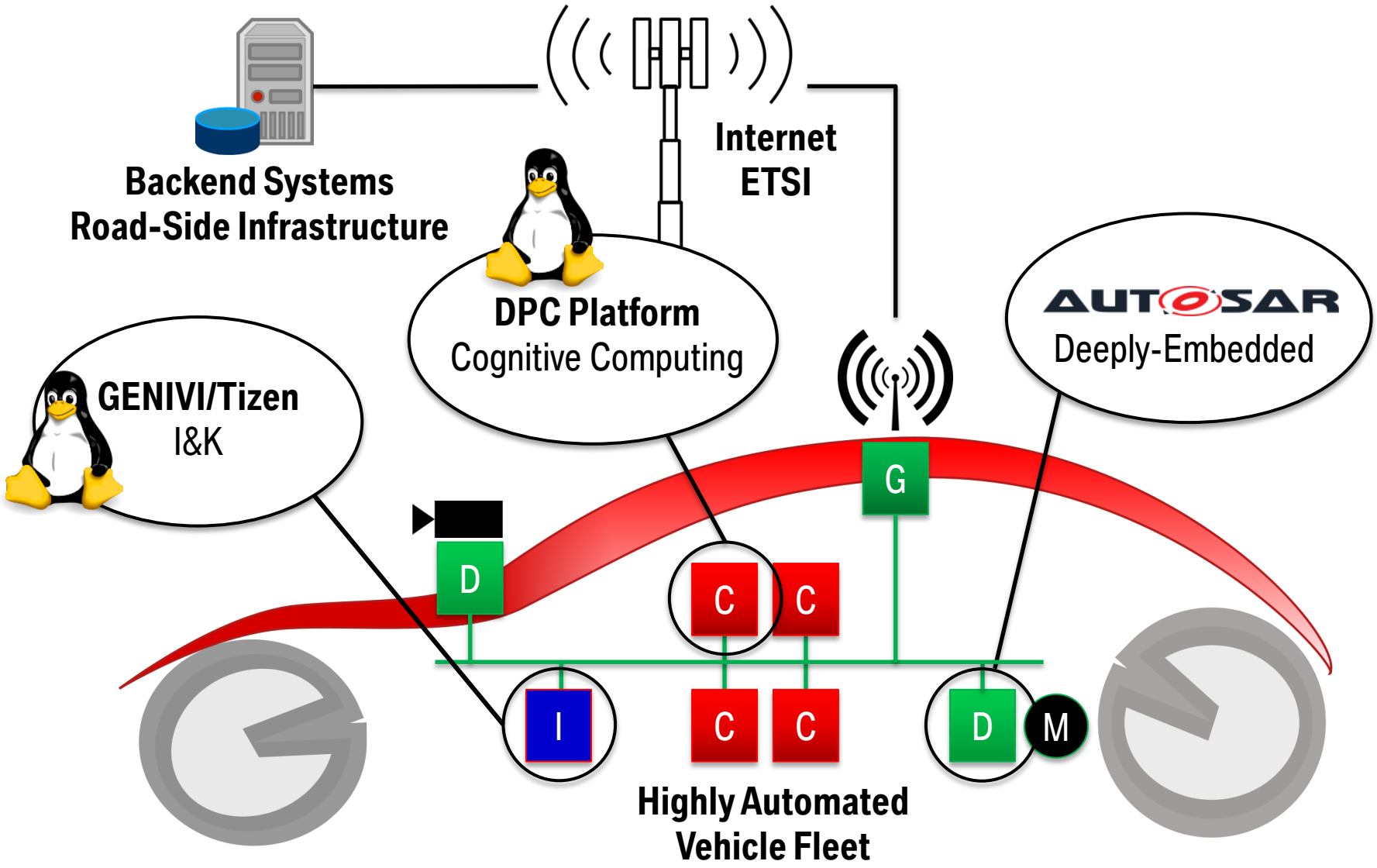
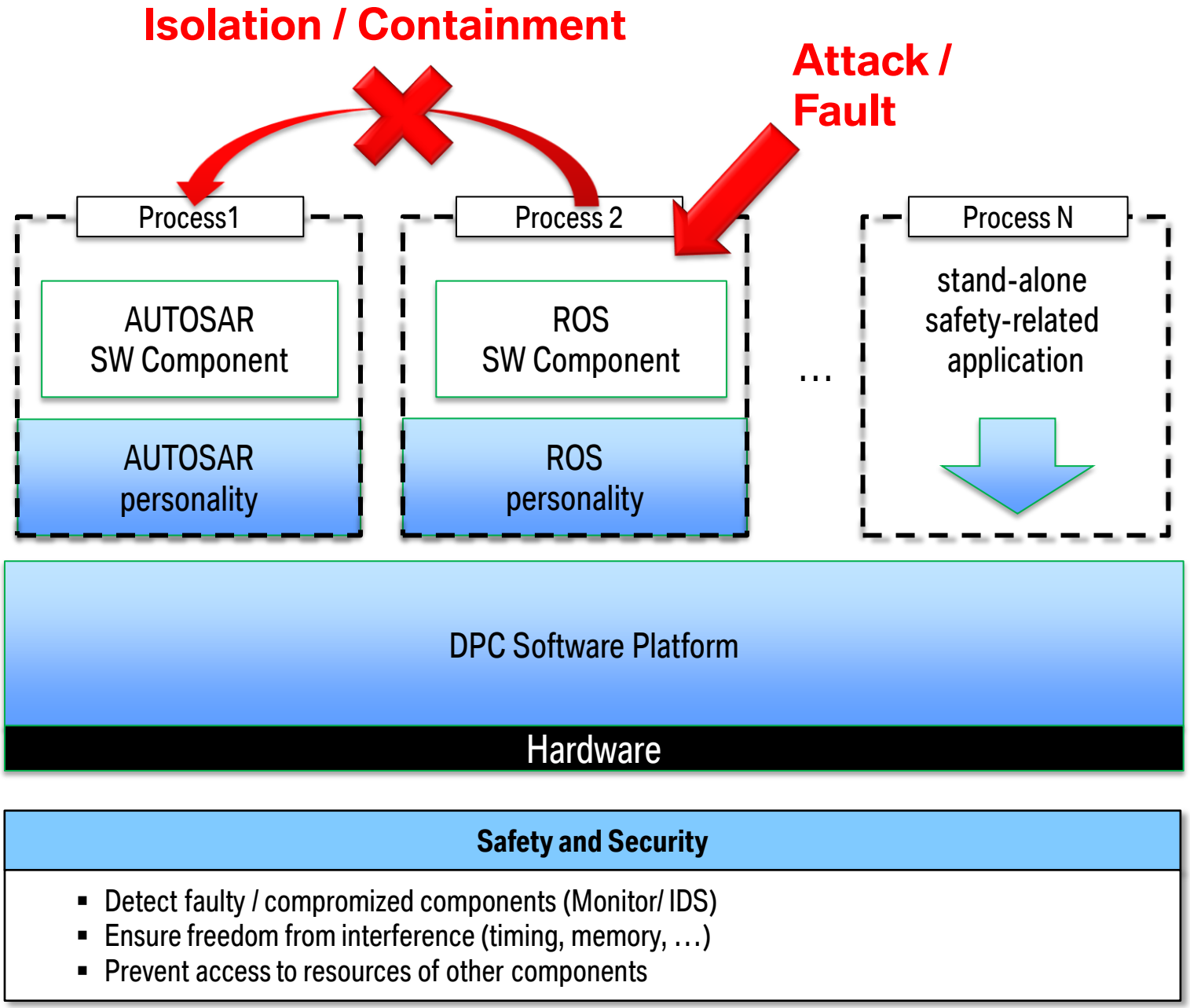
BMW Car IT GmbH, 15.10.2014

PROCESS ISOLATION FOR AUTONOMOUS DRIVING

BMW
GROUP
BMW Car IT GmbH

OPENSPACE PROJECT: VEHICLE E/E LANDSCAPE




Isolation / Containment
Attack / Fault
Process1
Process 2
Process N
AUTOSAR SW Component
ROS SW Component
stand-alone safety-related application
...
AUTOSAR personality
ROS personality
DPC Software Platform
Hardware
Safety and Security
Detect faulty / compromized components (Monitor/ IDS)
Ensure freedom from interference (timing, memory, …)
Prevent access to resources of other components

VIRTUALISATION VS. PROCESS ISOLATION

Full Virtualization

- virtual hardware resources
- separate os instance per partition
- strongest possible isolation

+ strong isolation
- more swc than cores
- resource overhead
- less flexible

Process Isolation

- virtual address space
- shared os resources
- highest resource efficiency

+ sufficient isolation
+ resource efficiency
- no off-the-shelf solution

OS Level Virtualization

- portability among distributions
- migration of running containers

+ large communities
- slight runtime overhead

KNOWN TECHNOLOGY

Vanilla Kernel Features

- users and groups (DAC, access control)
- ACLs (POSIX.1e, fs access control)
- capabilities (POSIX.1e, permission management)
- rlimits (kind of resource control)
- LSM SELinux / SMACK / … (MAC)
- cgroups (resource control)
- SECCOMP (syscall access control)
- NUMA support (performance isolation)
- SCHED_DEADLINE (timing isolation)
- UIO (isolation for device drivers)
- namespaces (process-level virtualization)
- device mapper (fs integrity / encryption)
- netfilter / iptables (network resource control)

Containers

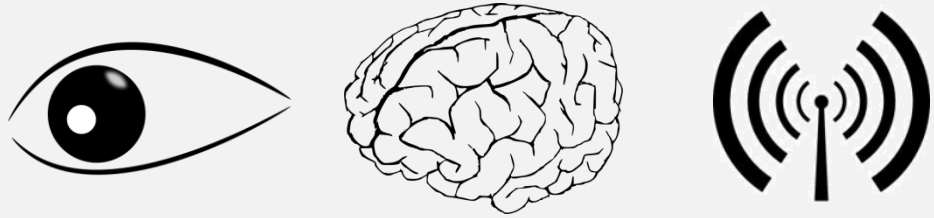
- linux containers (LXC, os-level virtualization)
- Docker (single application container)
- OpenVZ (kernel patches)
- Android security concept
- Tizen security concept

Research

- memguard (memory bandwidth reservation)
- traffic tainting and filtering

MORE? EXPERIENCES? THOUGHTS?

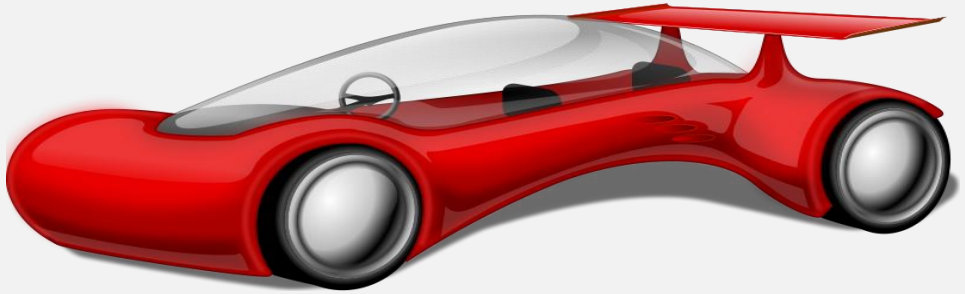
AUTOMOTIVE COMPUTING



backend
road-side

advanced driver assistance, automated driving

Cognitive Software



manual driving, driver assistance, active safety

Control Software

Control Software

- state machine + controller
- mature state-of-the-art
- static software structure and configuration
- automotive microcontrollers

Cognitive Software

- dynamic models + AI
- rapidly evolving technology
- dynamic software structure and configuration
- high performance mainstream HW