PROCESS ISOLATION FOR AUTONOMOUS DRIVING
OPENSPACE PROJECT: VEHICLE E/E LANDSCAPE

Backend Systems
Road-Side Infrastructure

Internet ETSI

DPC Platform
Cognitive Computing

AUTOSAR
Deeply-Embedded

GENIVI/Tizen
I&K

Highly Automated
Vehicle Fleet

BMW Car IT GmbH, 15.10.2014
Isolation / Containment

AUTOSAR SW Component

ROS SW Component

DPC Software Platform

Hardware

Safety and Security

- Detect faulty / compromised components (Monitor/IDS)
- Ensure freedom from interference (timing, memory, …)
- Prevent access to resources of other components

BMW Car IT GmbH, 15.10.2014
VIRTUALISATION VS. PROCESS ISOLATION

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

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

OS Level Virtualization
- portability among distributions
- migration of running containers

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

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

+ 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

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

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

advanced driver assistance, automated driving

manual driving, driver assistance, active safety

backend road-side