SOAFEE

Red Hat's Path to Automotive Functional Safety and New Breakthroughs in Container Applications

姜垚 *Rose Chiang*

Representative of Greater China, In-Vehicle OS
at Red Hat

Nov.12, 2025

SOAFEE

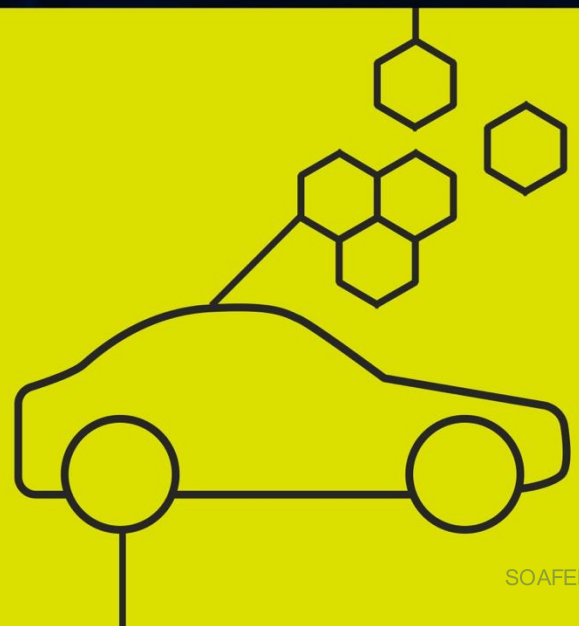
Topics :

The Importance of Functional Safety Linux

Container ASIL-B Implementation

Advantages of FFI-Isolated ADAS Applications

Ecosystem in Automotive community



SOAFEE

The Importance of Functional Safety Linux

China's New ADAS Safety Framework: From Guidance to Enforcement

Strategic shift

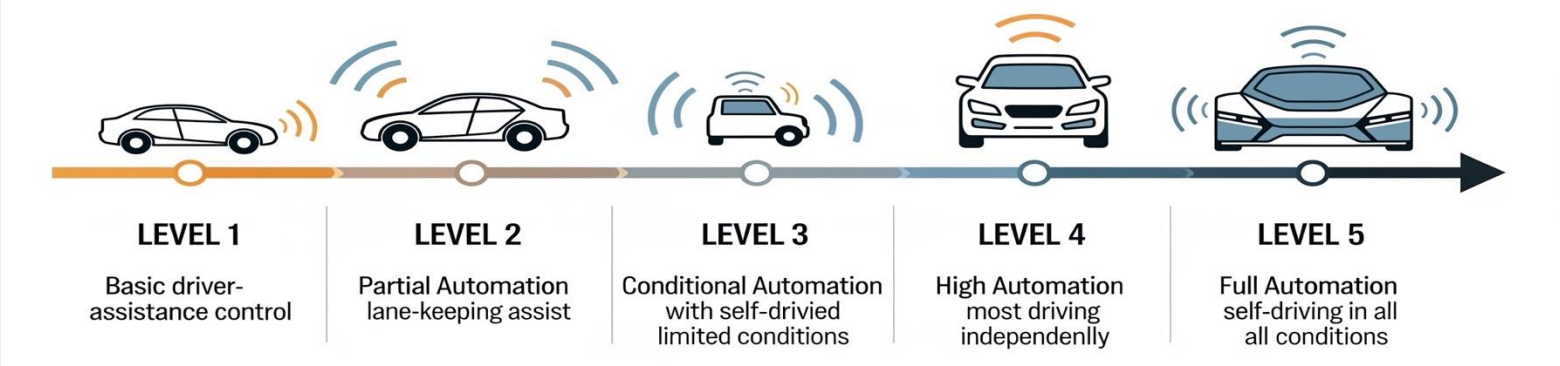
- Draft → Regulatory Directive
- Type Approval = Safety Case
- Evidence-Based Verification

Safety baseline

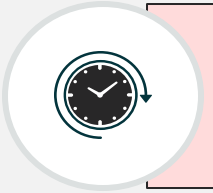
- FuSa + SOTIF Focus
- Baseline ASILs Definition
- Requires Full Traceability

Beyond Security

- Cybersecurity (GB 44495 / UN R155 / ISO 21434)
- Secure OTA Updates (GB 44496 / UN R156)
- Added Compliance Extensions for China



The changes that open-source Linux will bring to automotive

Features of Red Hat In-Vehicle OS	Help for OEMs
 Container	• Accelerate the release of new features and services. • Standalone applications can be written in multiple programming languages. • Application testing no longer requires a hardware testing platform.
 Faster time for market	• Increase market share and surpass competitors • Attract customers to the automotive ecosystem • Accelerate vehicle upgrade cycles
 A rich talent pool	• Compared to other proprietary operating systems, it's easier to recruit engineers with Linux experience, shortens engineer onboarding time, and requires higher levels of operating system knowledge and expertise.
 Cybersecurity	• Vulnerabilities are easier to discover and fix through the open-source community. • Red Hat Linux systems are trusted across various industries. • This reduces reputational risk for OEMs.

An open, FuSa-certified OS designed to lead local development and achieve global expansion.

Red Hat In-Vehicle Operating System

	FuSa certification	The base operating system is ISO 26262 ASIL-B certified and has been evaluated by exida.
	Faster access to global markets	Pre-certified infrastructure can speed up local approvals and global rollout.
	Globally recognized	Compliant with ISO 26262 ASIL-B standard, globally recognized.
	No limitation	An open, transparent, and vendor-neutral platform that enjoys global trust.

Tailor-made to meet the specific needs of the automotive industry

Red Hat
In-Vehicle
Operating System

Open | ASIL-B | Secure

Real-time functionality

Fasten boot

Mixed-Criticality
FFI

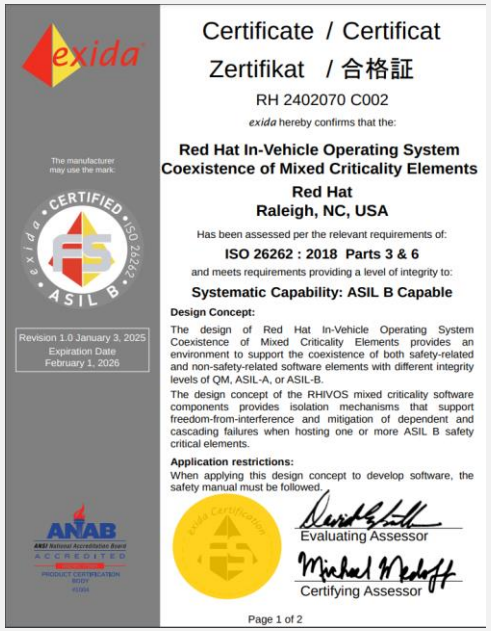
Hardware support diversity

Multiple application scenarios

Modern software development

RHIVOS FuSa Certification - Get !


Certificate / Certificat
Zertifikat / 合格証
RH 2402070 C001
exida hereby confirms that the:
Red Hat In-Vehicle Operating System GLIBC Mathematics Library
Red Hat Inc.
Raleigh, NC, USA
Has been assessed per the relevant requirements of:
ISO 26262 : 2018 Parts 2, 4, 6, 8, and 9
and meets requirements providing a level of integrity to:
Systematic Capability: ASIL B Capable
Safety Function:
The RHIVOS glibc Math Library functions execute correctly per their specified man pages.
Application restrictions:
The tool must be used per the User Manual requirements and the assumed workflow described on the reverse side.
Revision 1.0 June 14, 2024
Surveillance Audit Due
July 1, 2025
Evaluating Assessor
Certifying Assessor


Certificate / Certificat
Zertifikat / 合格証
RH 2402070 C002
exida hereby confirms that the:
Red Hat In-Vehicle Operating System Coexistence of Mixed Criticality Elements
Red Hat
Raleigh, NC, USA
Has been assessed per the relevant requirements of:
ISO 26262 : 2018 Parts 3 & 6
and meets requirements providing a level of integrity to:
Systematic Capability: ASIL B Capable
Design Concept:
The design of Red Hat In-Vehicle Operating System Coexistence of Mixed Criticality Elements provides an environment to support the coexistence of both safety-related and non-safety-related software elements with different integrity levels of QM, ASIL-A, or ASIL-B.
The design concept of the RHIVOS mixed criticality software components provides isolation mechanisms that support freedom-from-interference and mitigation of dependent and cascading failures when hosting one or more ASIL B safety critical elements.
Application restrictions:
When applying this design concept to develop software, the safety manual must be followed.
Revision 1.0 January 3, 2025
Expiration Date
February 1, 2026
Evaluating Assessor
Certifying Assessor
Page 1 of 2


Certificate / Certificat
Zertifikat / 合格証
RH 2402070 C003
exida hereby confirms that the:
Red Hat In-Vehicle Operating System
Red Hat, Inc.
Raleigh, NC, USA
Has been assessed per the relevant requirements of:
ISO 26262 : 2018 Parts 2, 6, 7, 8, & 9
and meets requirements providing a level of integrity to:
Systematic Capability: ASIL B Capable
Product Details:
Red Hat In-Vehicle Operating System is an automotive platform that supports the coexistence of QM and ASIL B software within the same OS image. It initializes services and applications at startup, ensures freedom from interference through containerization, memory protection and isolation features, manages CPU time allocation to mitigate temporal interference and applies per-process access control policies to restrict access to files and system calls.
See the Assessment Report for detailed Safety Claims.
Application restrictions:
When using Red Hat In-Vehicle Operating System to develop software, the safety guidance must be followed and components used for safety related applications must match those in the guidance.
Revision 1.2 May 16, 2025
Expiration Date
June 1, 2026
Evaluating Assessor
Certifying Assessor
Page 1 of 2

- Next steps :

  Further expand the functionality available to customers in secure applications.

Math ✓

This proves that the Red Hat method is feasible for component authentication.
Complete

Mixed Criticality ✓

Focus on the key elements of FFI-related arguments.

Certified: Jan 3 2025

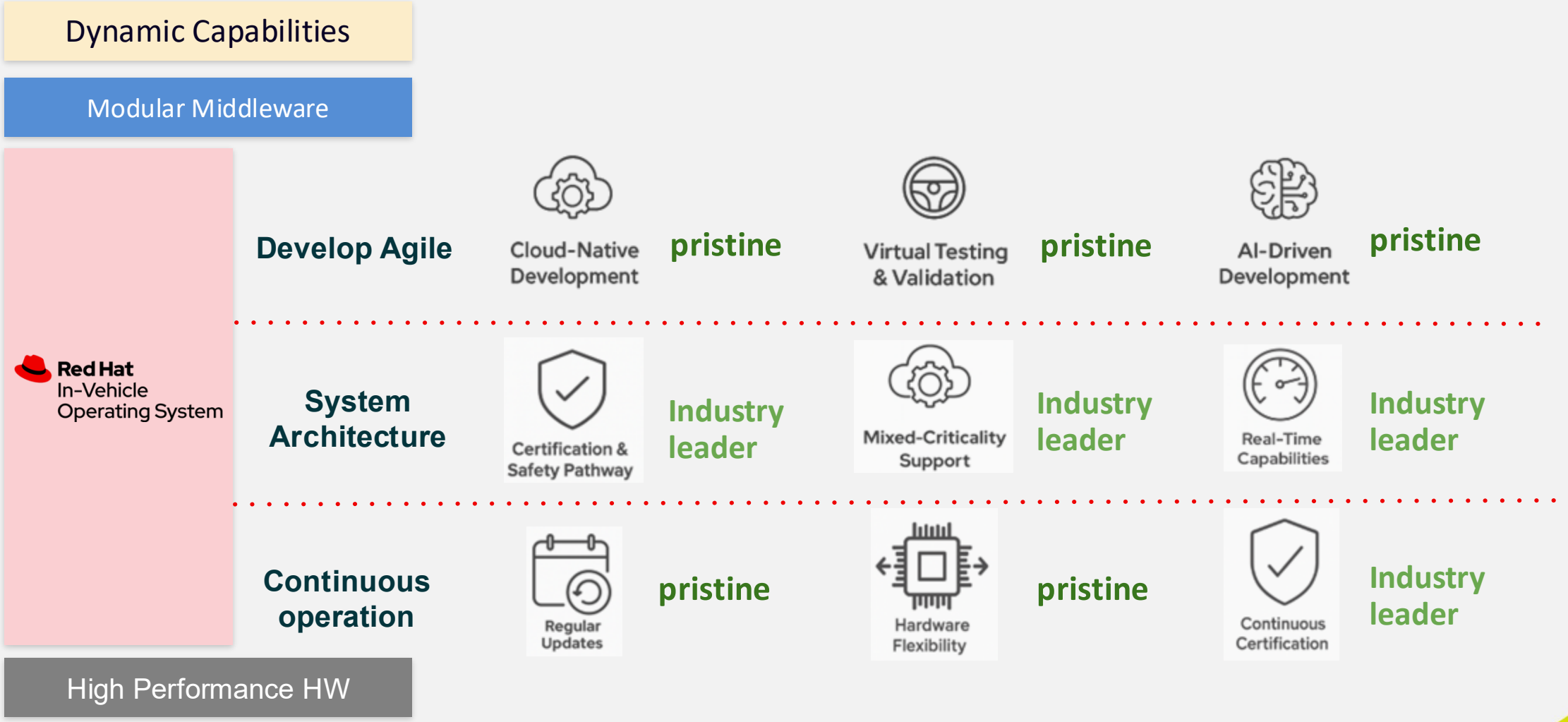
Product Certification ✓

Certified to meet the ASIL-B safety element standard of ISO 26262, version 2, 2018.

1st Certified: May 13 2025

2nd Certified: Oct 24 2025

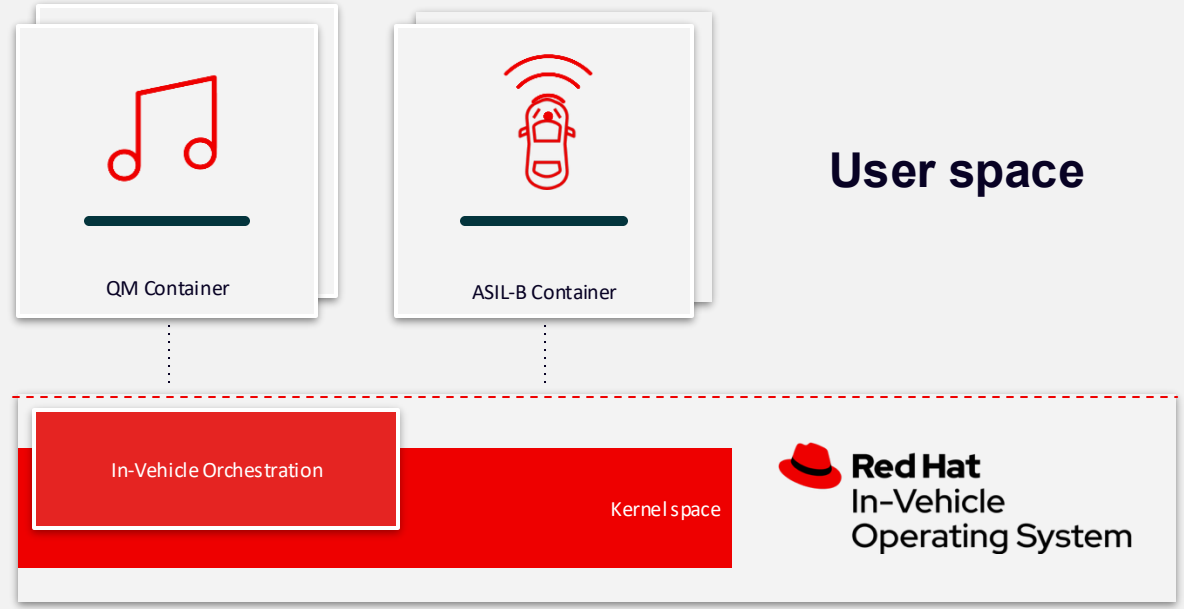
Red Hat In-Vehicle OS, our advantages and key points of argumentation in OS standards



SOAFEE

Container ASIL-B Implementation

Functional safety container solution



bluechi

podman

Container running without a daemon

- A fast, efficient, and lightweight solution
- Based on Red Hat's lightweight crun runtime
- The container is a generic interface for OCI.
- Integrates with functional safety and systemd for monitoring and performance allocation

Native Red Hat Linux technology

- Container safety technology: Process monitoring and resource allocation in functional safety certification

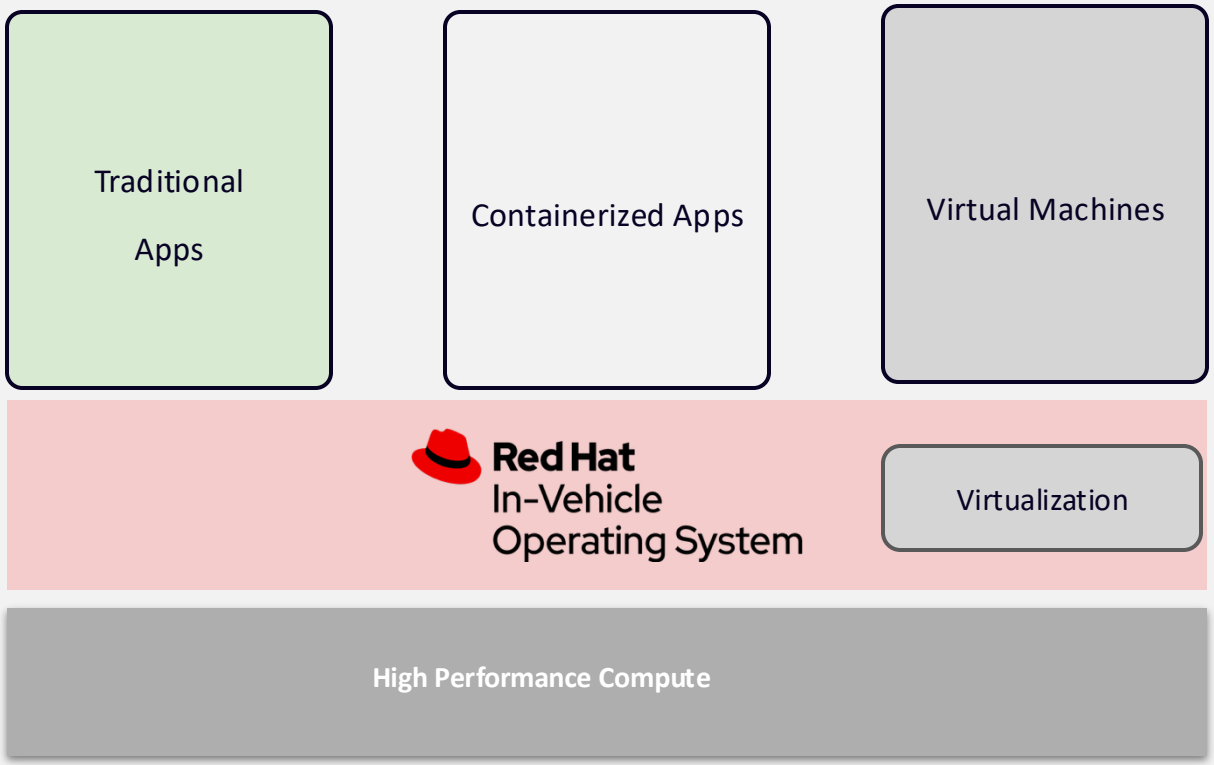
FuSa

- Third-party ISO26262 ASIL-B functional safety certification

Multi-point container management – BlueChi

- Red Hat's systemd simplifies cross-platform multi-point management.(container, VM, bare metal…)
- Open Source Eclipse SDV https://github.com/containers/bluechi

Red Hat supports a seamless transition to containerized workloads.

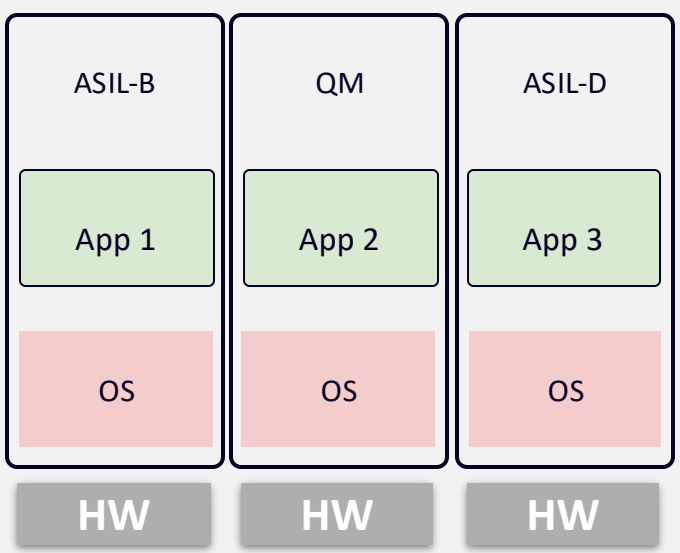


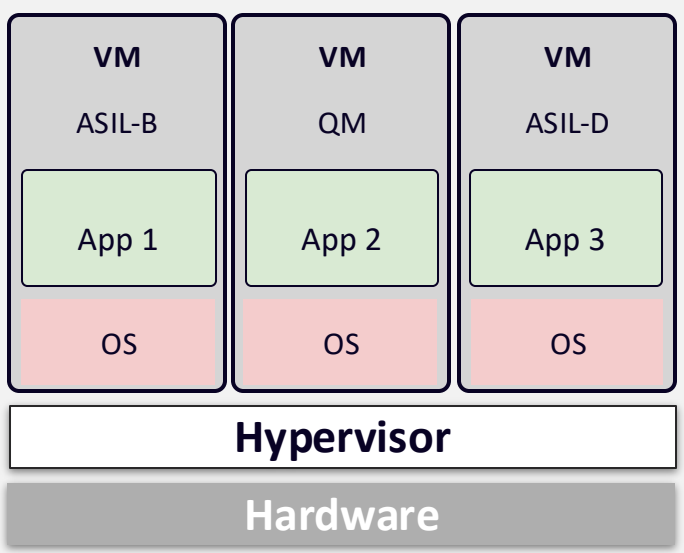
Easily migrate existing applications.
Cloud-native containers enable this :

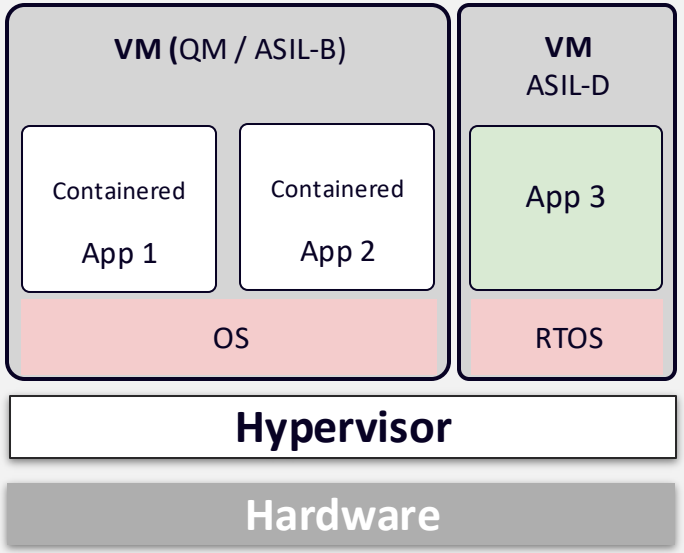
- Modular, fine-grained updates
- Accelerate development
- Optimize resource utilization
- Enhance security and isolation
- Improve portability and consistency

Isolate applications more securely.

Evolution of automotive architecture







Past – Independent Hardware

- Single-purpose hardware
- Complex and costly update process
- Isolated development
- Limited reusability

Today – Hypervisor Virtual Machine

- High resource utilization
- Complex architecture
- Strong hardware-level isolation
- Reduced flexibility in updates

The Future – Flexible Applications of Containers + Virtual Machines

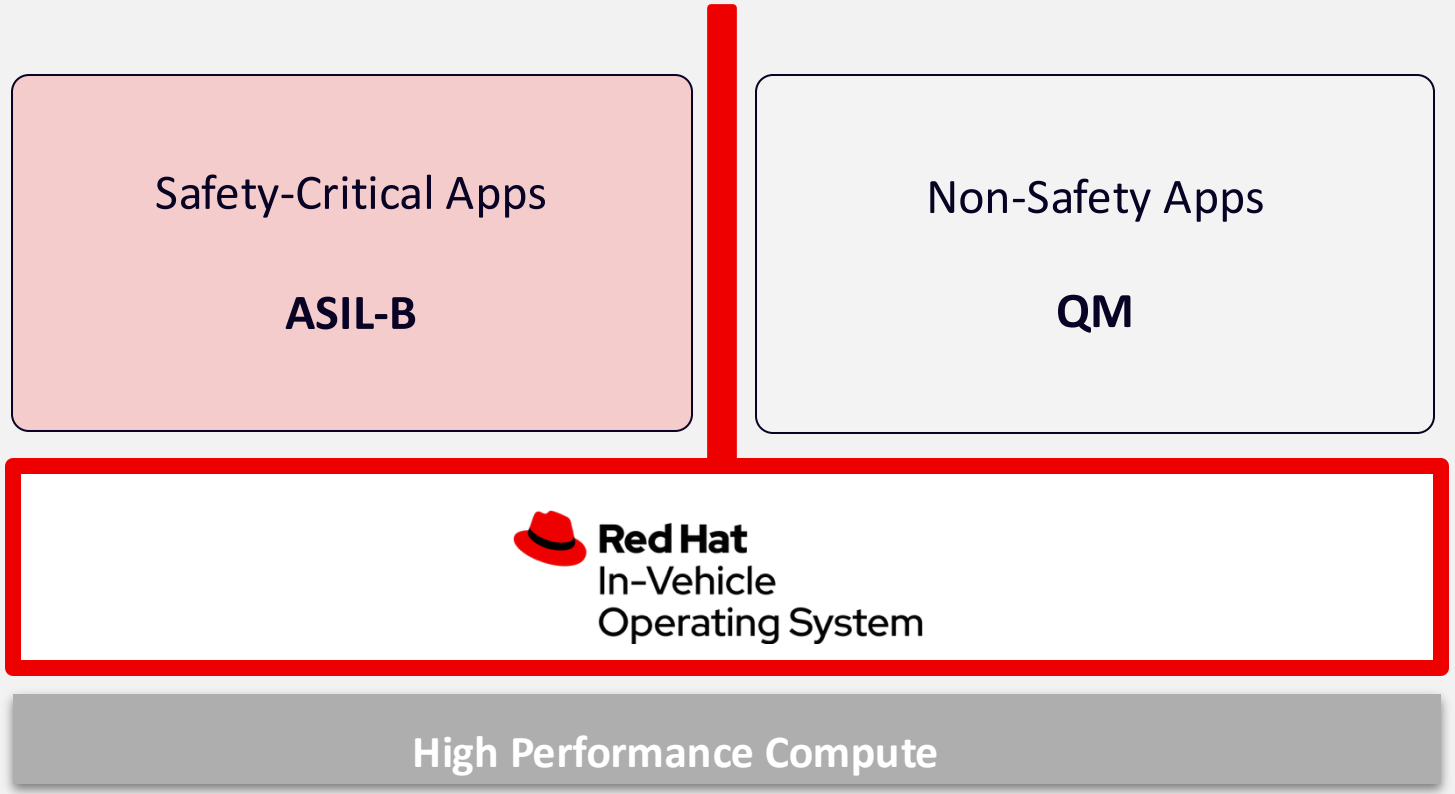
- Efficient resource utilization
- Simpler architecture
- Greater flexibility
- Rapid deployment and seamless OTA updates

SOAFEE

Advantages of FFI-Isolated ADAS Applications

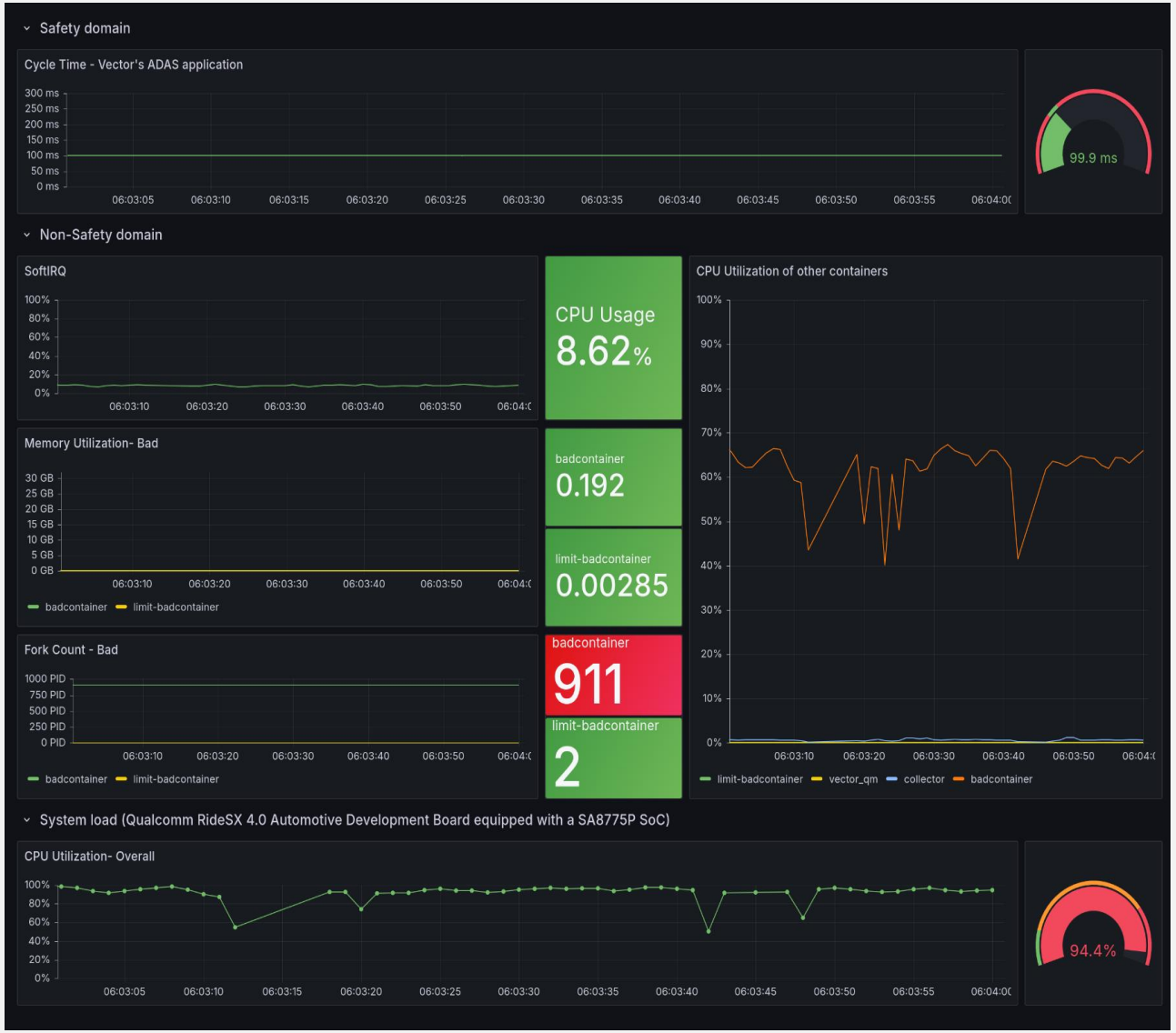
Red Hat In-Vehicle OS has passed mixed-criticality certification

- ✓ Temporal isolation
- ✓ Resource isolation
- ✓ Spatial isolation



- ❑ Simplify architecture
- ❑ Reduce engineering investment
- ❑ Lower system costs
- ❑ Continuously update

RHIVOS Demo Show



ASIL-B area:

Objective: Maintain ADAS process cycle time at 100ms

QM area:

Demonstration: Creating various disturbances and high-intensity loads to generate container failure interference.

Highlights: :

- The overall CPU load is close to 90% or higher, while the execution time of processes in the functional safety region remains unchanged at 100ms.
- Failure in the QM region does not interfere with the operation of the functional safety region, thus achieving safer ADAS protection.

SOAFEE

Ecosystem

Current Automotive Community Engagements

CentOS Automotive SIG

Curator of the Automotive Stream Distribution, upstream for the Red Hat In-Vehicle OS

Eclipse SDV WG | S-CORE

Industry consortium developing a software ecosystem for software-defined vehicles

Scalable Open Arch for Embedded Edge

Industry consortium developing an open architecture for software-defined vehicles

Collaborative alliance among SDV orgs: Eclipse SDV, SOAFEE, COVESA, AUTOSAR

Connected Vehicle Systems Alliance

Connected Vehicle specifications including Vehicle Signal Specification (VSS)

Enabling Linux In Safety Applications

Functional safety code and evaluation projects within the Linux kernel and ecosystem

Standards process development for functional safety in vehicles: ISO 26262

Autoware Foundation

Open AD project based on ROS2, supported by CentOS AutoSD and SOAFEE

WEF SDV Task Force

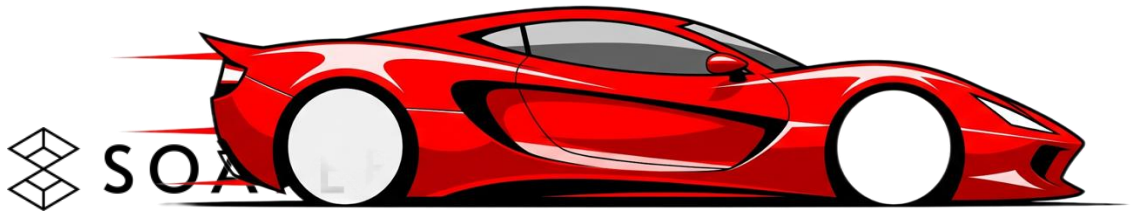
Global research project formed by WEF in conjunction with BCG and industry players

FuSa Linux white Paper released in Sep. 2024

Scalable Open Architecture for Embedded Edge Project (SIG)

https://soafee.io

- Special Interest Group within Arm
- Collaboration on automotive software specifications & reference implementations for modern cars
- Strong collaboration on SDV designs, including OS, ADAS, and hypervisors, direct relationship with Eclipse SDV
- Governance groups so far:
  - Governing Body (GB)
  - Marketing/GTM Steering Committee (MSC)
  - Technical Steering Committee (TSC)
    - Architecture WG
      - System Architecture WG
      - Cloud Native Dev WG
      - Cloud Native Tooling WG
    - Reference Implementation WG
- First specification release coming Oct 2022



Thank You

Rose Chiang
rchiang@redhat.com