

The Application of Micro-kernel Based Operating System in Cross-domain Computing for Intelligent Vehicles

Ding Wang

Black Sesame Technologies Co., Ltd

2023/09/21

What makes automotive software special?

**Safety
Criticality**

**Real-time
Requirements**

**Complex
Systems**

**Regulatory
Compliance**

**Long Product
Lifecycles**

**Environmental
Constraints**



What is Functional Safety?

ISO 26262

1. Vocabulary		
2. Management of functional safety		
2-5 Overall safety management	2-6 Project dependent safety management	2-7 Safety management regarding production, operation, service and decommissioning
3. Concept phase		
3-5 Item definition	4. Product development at the system level	
3-6 Hazard analysis and risk assessment	4-5 General topics for the product development at the system level	4-7 System and Item Integration and testing
3-7 Functional safety concept	4-6 Technical safety concept	4-8 Safety validation
7. Production, operation, service and decommissioning		
7-5 Planning for production, operation, service and decommissioning		
7-6 Production		
7-7 Operation, service and decommissioning		
12. Adaptation of ISO 26262 for motorcycles		
12-5 General topics for adaptation for motorcycles	5. Product development at the hardware level	
12-6 Safety culture	5-5 General topics for the product development at the hardware level	6. Product development at the software level
12-7 Confirmation measures	5-6 Specification of hardware safety requirements	6-5 General topics for the product development at the software level
12-8 Hazard analysis and risk assessment	5-7 Hardware design	6-6 Specification of software safety requirements
12-9 Vehicle integration and testing	5-8 Evaluation of the hardware architectural metrics	6-7 Software architectural design
12-10 Safety validation	5-9 Evaluation of safety goal violations due to random hardware failures	6-8 Software unit design and implementation
	5-10 Hardware integration and verification	6-9 Software unit verification
		6-10 Software integration and verification
		6-11 Testing of the embedded software
8. Supporting processes		
8-5 Interfaces within distributed developments	8-9 Verification	8-14 Proven in use argument
8-6 Specification and management of safety requirements	8-10 Documentation management	8-15 Interfacing an application that is out of scope of ISO 26262
8-7 Configuration management	8-11 Confidence in the use of software tools	8-16 Integration of safety-related systems not developed according to ISO 26262
8-8 Change management	8-12 Qualification of software components	
	8-13 Evaluation of hardware elements	
9. Automotive safety integrity level (ASIL)-oriented and safety-oriented analyses		
9-5 Requirements decomposition with respect to ASIL tailoring	9-7 Analysis of dependent failures	
9-6 Criteria for coexistence of elements	9-8 Safety analyses	
10. Guidelines on ISO 26262		
11. Guidelines on application of ISO 26262 to semiconductors		

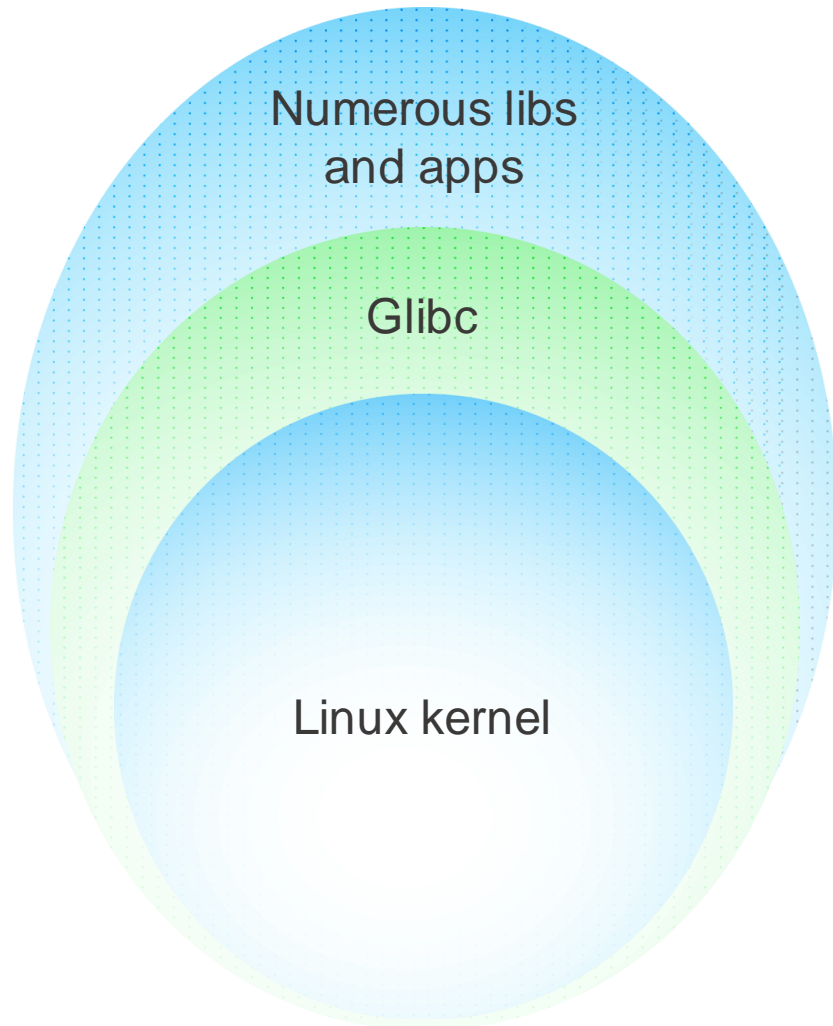
ASIL Automotive Safety Integrity Level

Severity	Exposure	Controllability		
		C1	C2	C3
S1	E1	QM	QM	QM
	E2	QM	QM	QM
	E3	QM	QM	A
	E4	QM	A	B
S2	E1	QM	QM	QM
	E2	QM	QM	A
	E3	QM	A	B
	E4	A	B	C
S3	E1	QM	QM	A
	E2	QM	A	B
	E3	A	B	C
	E4	B	C	D

About \$10-100 cost per LOC for ASIL-D certification

Hypervisor

Nobody can check all these codes for functional safety



Numerous libs and apps

systemd: 750,338 LOC

libc++: 570603LOC

ffmpeg: 1,391,908LOC

OpenCV: 2,185,540LOC

GNU C Library

has had 40,366 commits made by 724 contributors

representing 1,423,198 lines of code

<https://openhub.net/p/glibc>

Kernel

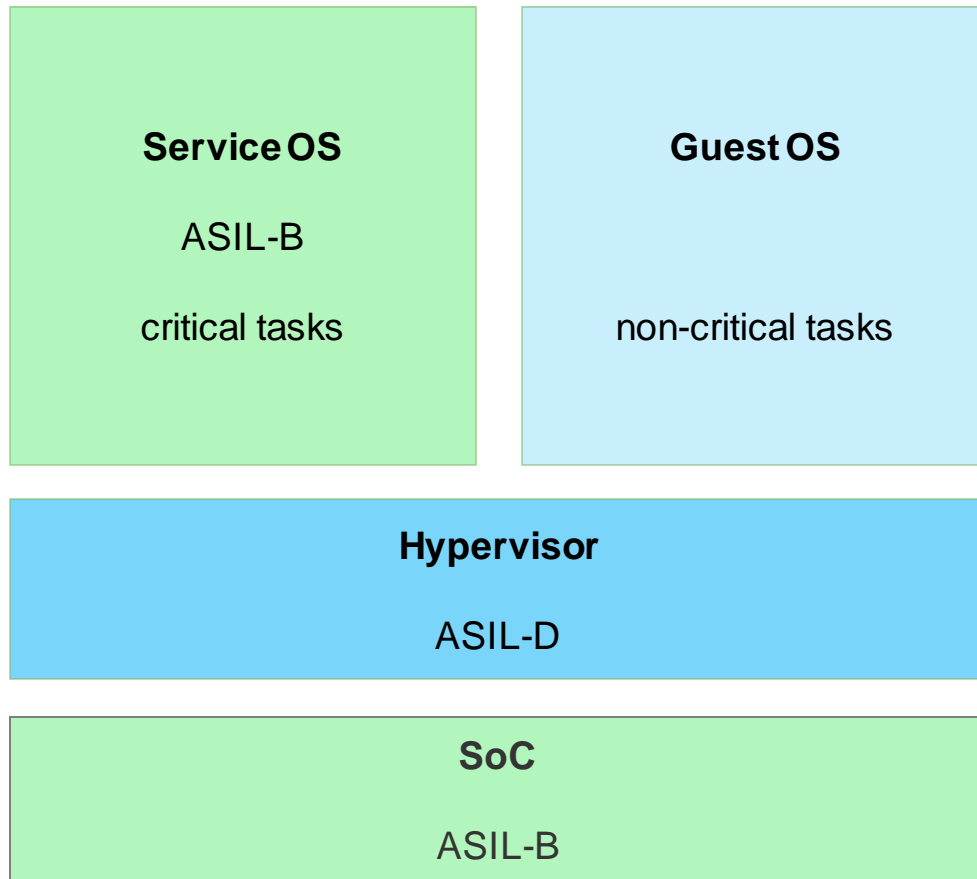
has had 1,197,344 commits made by 26,958 contributors

representing 34,199,731 lines of code

<https://openhub.net/p/linux>

Dual-Kernel Solution

◆ A system engineering solution

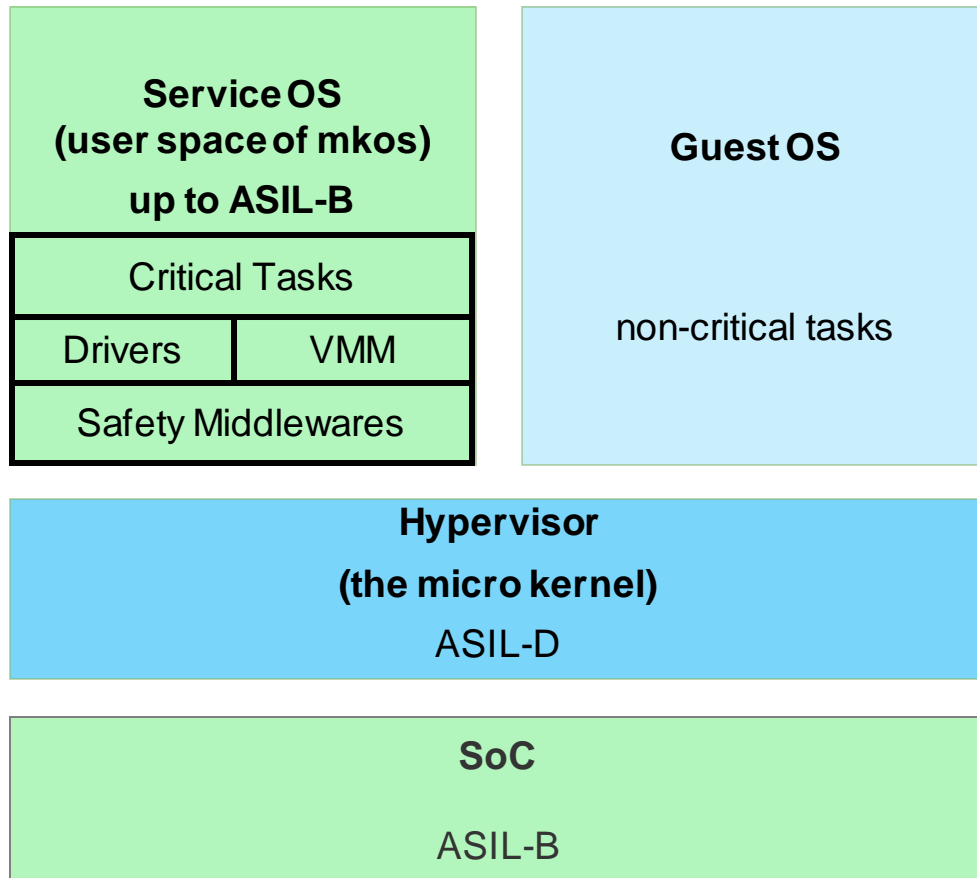


- Hypervisor
 - up to ASIL-D
 - doing kernel switch and cross OS communication
- Service OS
 - upto ASIL-B, maybe a ASIL-D kernel and ASIL-B middlewares
 - running critical tasks
- Guest OS
 - can be Linux
 - for non-critical tasks

The whole system is achieved ASIL-B.

Micro-kernel based hypervisor

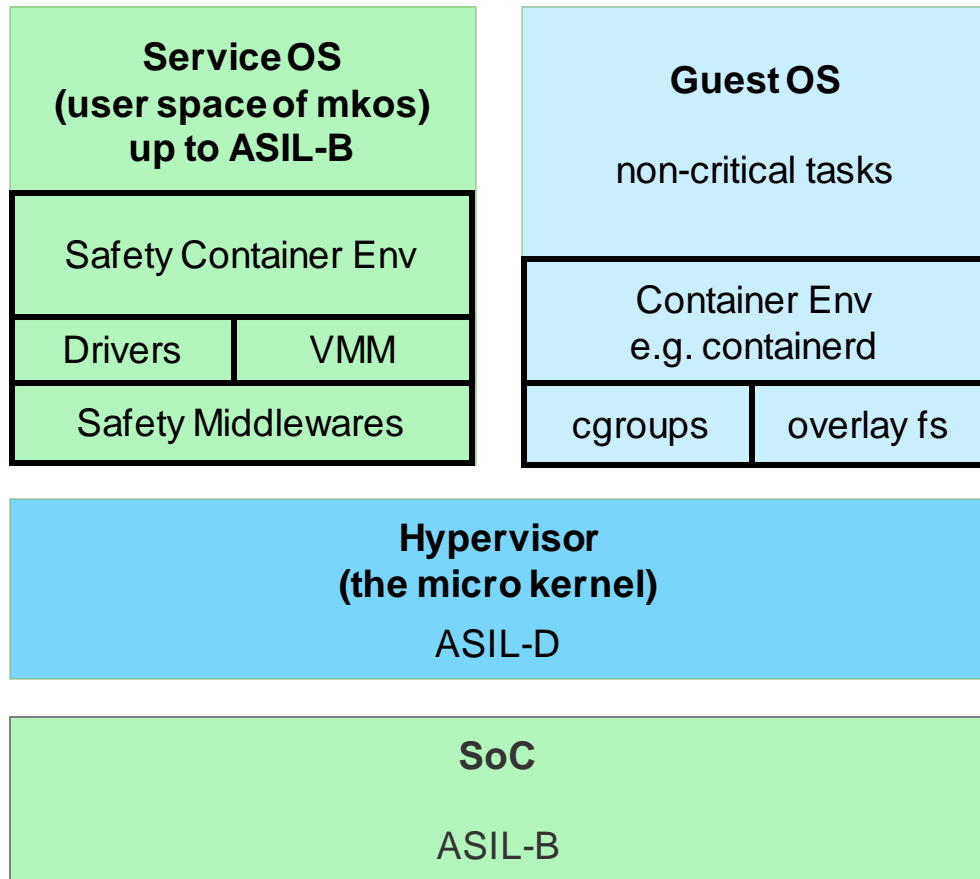
Micro-kernel as hypervisor and SOS



- Hypervisor
 - the micro kernel itself.
- Service OS
 - not the VM, but just the user space of the micro kernel OS.
- Guest OS
 - a VM running on micro kernel OS.
 - for non-critical tasks
- Advantages
 - strengthen SOS, for realtime, reliability, etc.
- Disadvantages
 - weaken GOS, for schedule, latency, etc.

Container support

Container support in SOS and GOS



- Service OS
 - a safety container environment
- Guest OS
 - standard container environment

With container support, the architecture requirement of SOAFEE can be met.

Applications can be developed/tested/deployed in container mode.



Technical Trends

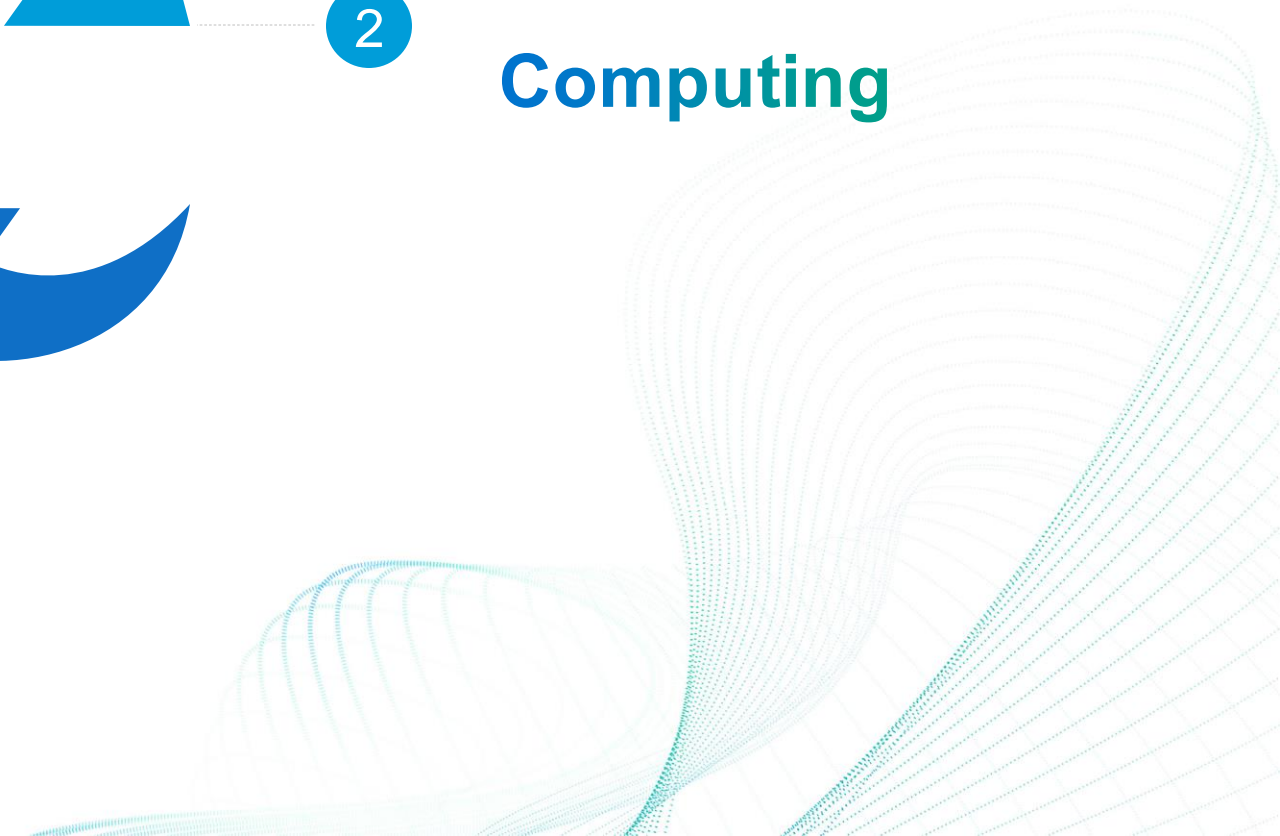
**Centralized
Computing**

1



2

**Distributed
Computing**



Product | Cross-domain SoCs – Wudang Series

The first cross-domain computing platform for intelligent vehicles in China
and target towards **cross-domain computing scenarios**.

(launched in Apr. 2023, sample deliveries are planned for 2023)

Black Sesame Technologies
WUDANG SERIES
C1200
Cross-domain Computing Platform for Intelligent Vehicle

黑芝麻智能
BLACK SESAME
TECHNOLOGIES

C1200

A0XX AAA0000001A0
0101 FBA Q1

The 1st automotive grade cross domain computing platform to integrate multiple functions

Cross-domain Computing Platform
WUDANG SERIES

Advantages of
C1200



Innovative	Accurate	Powerful	Highest
fusion architecture	market positioning	family product platform	automotive grade requirements

Wudang Series **C1200**

The Industry Benchmark of Product Innovations



- Integrate multifunction in one SoC
- Maintain large amount of data exchanged efficiently
- Reuse software assets to a maximum extent
- Increase safety level
- Reduce the number of components in the system

Cross-Domain Computing

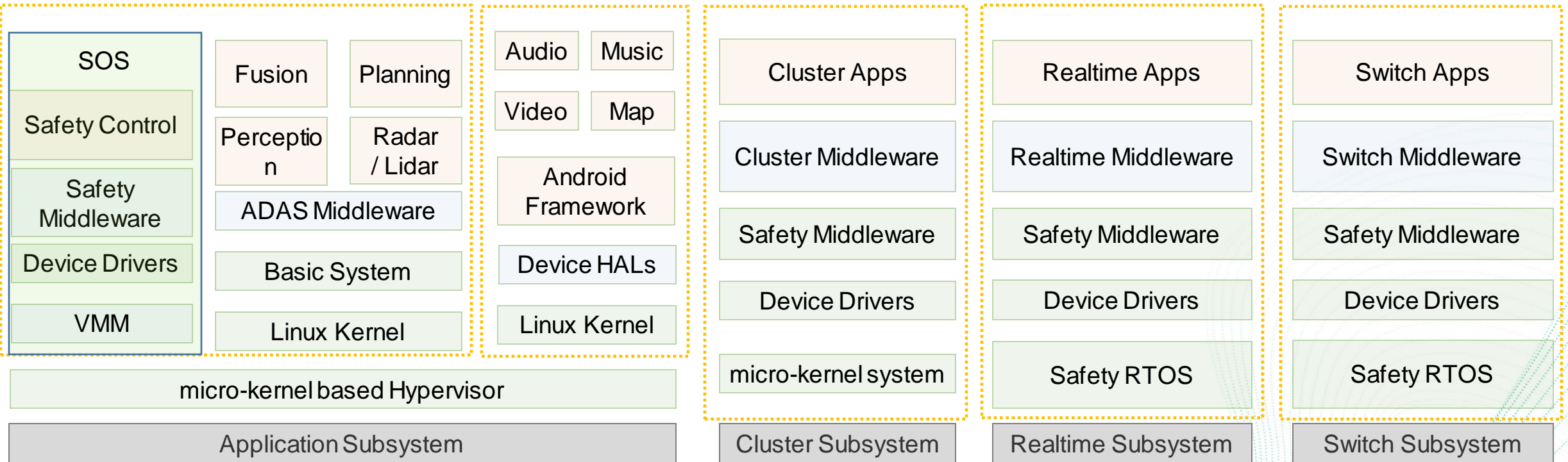
ADAS Domain
ASIL-B

IVI Domain

Cluster Domain
ASIL-B

Realtime Domain
ASIL-D

Switch Domain
ASIL-B/D



Thanks



**BLACK
SESAME**
TECHNOLOGIES