

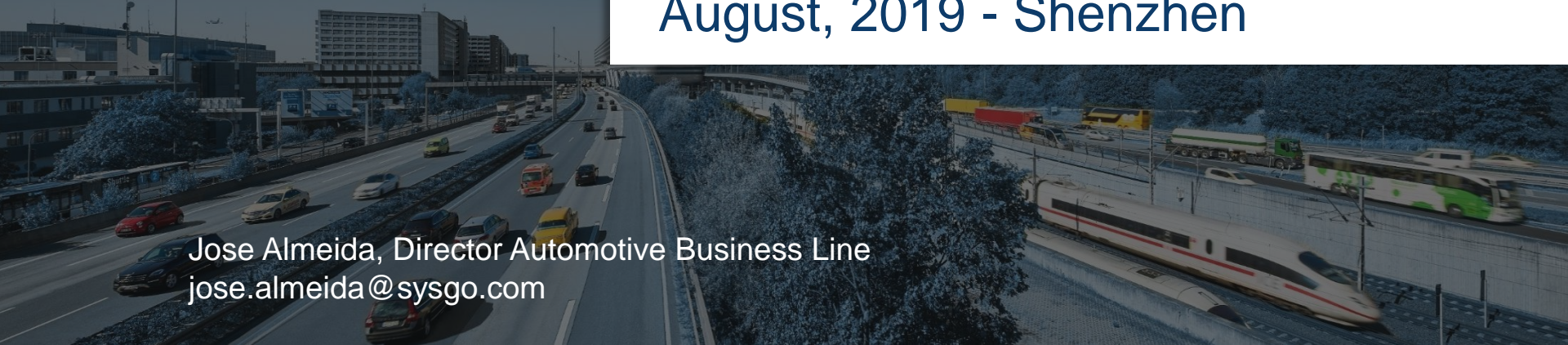


# Autonomous Driving Safety & Security Challenges

SAE-AWC

August, 2019 - Shenzhen

Jose Almeida, Director Automotive Business Line  
[jose.almeida@sysgo.com](mailto:jose.almeida@sysgo.com)



## DEVELOPING LOCALLY ACTING GLOBALLY

- SYSGO is the leading European operating system vendor for embedded systems.
- As a trusted advisor, we provide Safe & Secure technologies and services to be part of high-end software solutions in any IoT device worldwide.
- Founded in 1991 – more than 25 years experience in certification of Safety-critical systems
- Member of the Thales Group



# PRODUCTS AND SERVICES

As the leading European manufacturer of embedded operating systems, we have supported Safety & Security-critical applications in the aerospace, automotive, railway and IIoT industries for more than 25 years. We work closely with our customers throughout their product life cycle.

## PikeOS®

Separation Kernel based RTOS with integrated and certified virtualization technology (Hypervisor)

## ELinOS

Industrial grade Linux Distribution for embedded systems with real-time extensions

## Board Support Packages

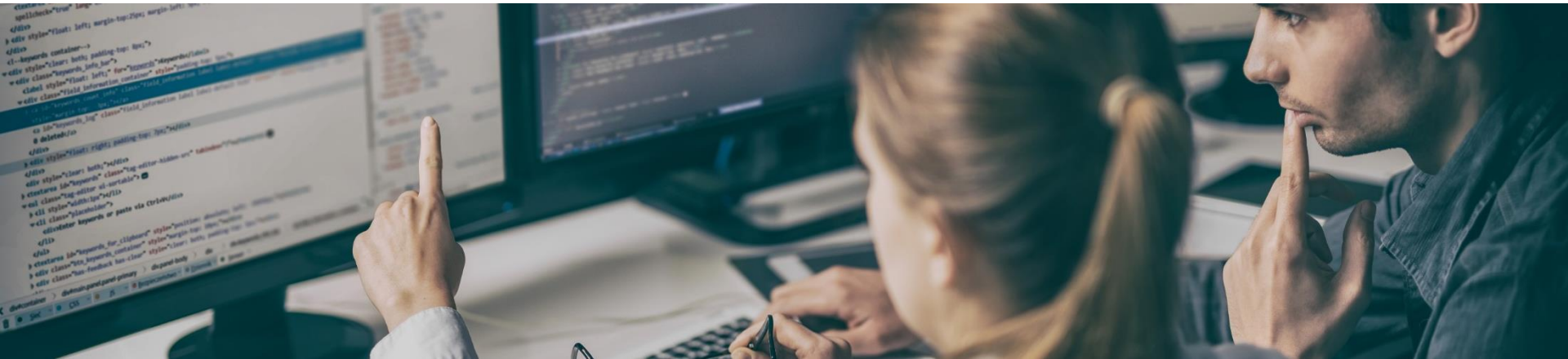
Adaptation to the selected architecture, board specific initialization and drivers

## Certification Kits

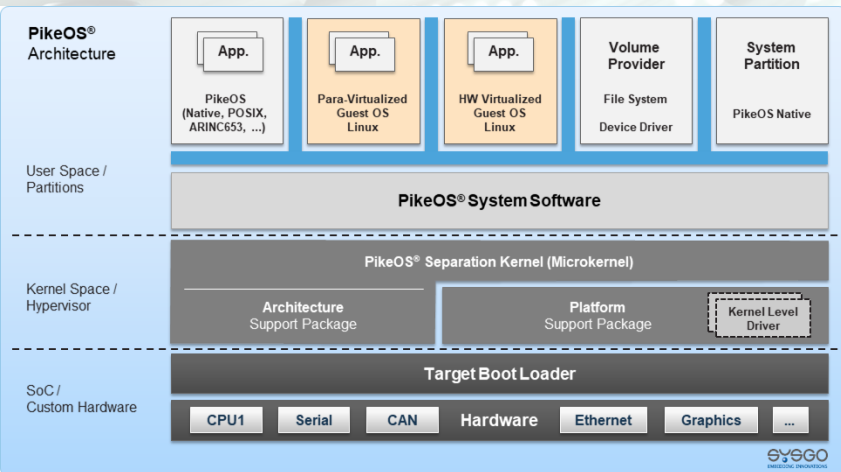
Extensive collection of certification artefacts for all major generic and industry-specific standards

## Professional Services

We make sure customers can optimize use our technology from prototyping to certification



**ITAR**  
· free ·



# PRODUCTS & SERVICES

## PikeOS®

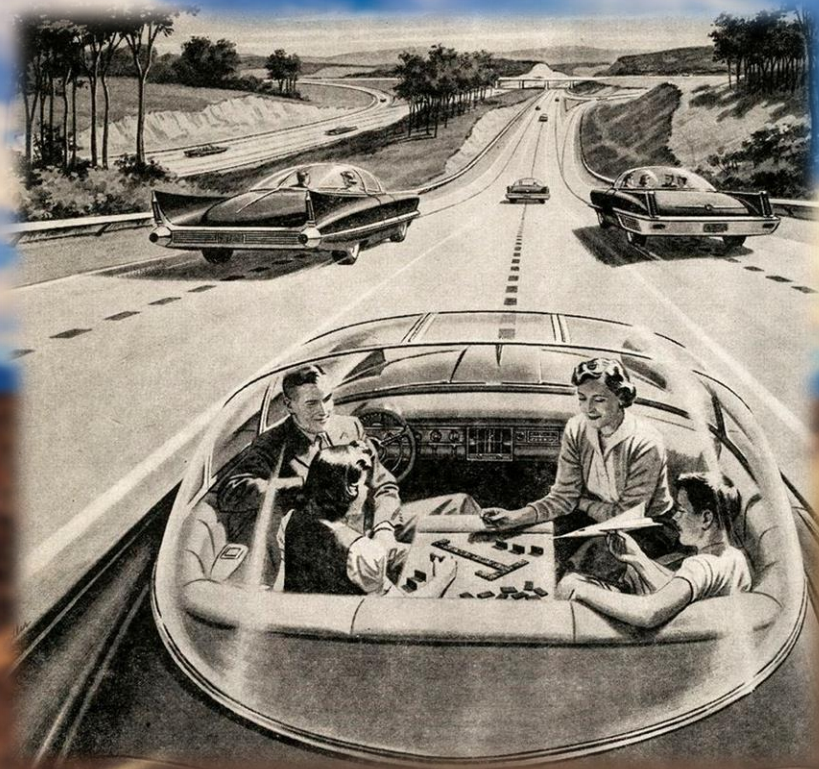
## EMBEDDED RTOS & HV

- **Hard Real-Time Operating System and Hypervisor**
  - With safe and secure virtualization, mixed criticality with multiple guest operating systems and highly portable, supporting all important CPU architectures
- **Guest Operating Systems**
  - Can run in parallel partitions on a single or multicore processor to serve specific use cases
- **Mixed Criticality**
  - Strict spatial and time partitioning
- **Eclipse-based CODEO**
  - A comprehensive integrated development environment supporting C/C++
- **Without any Export Restriction**
  - ITAR free




# AUTONOMOUS DRIVING THE VISION









NO TRUCKS OVER 4 1/2 TONS  
ON  580  
EAST OF GRAND AVE

 580 Alameda San Jose  
 80 San Francisco

 BUSES AND CARPOOLS ONLY  
5AM-10AM MON-FRI  
3PM-7PM  
San Francisco ONLY 

END CARPOOL LANE  
600 FEET 

 580 Oakland  
San Jose   

 80 San Francisco  
3 RIGHT LANES

LEFT LANE MUST BE LEFT

14 9

LEFT LANE MUST BE LEFT

EXIT 9 2



# AUTONOMOUS WHY'S

**Increase Safety (69%)**

**Road Capacity (65%)**

**Mobility, Stress (~50%)**

**Less Emission (31%)**



# MAIN CHALLENGES

**Safety Concerns /  
Fail Safe Concepts**

**Legal Restrictions**

**Cyber Security**



**NEW  
THINKING**





**NEW  
THINKING**

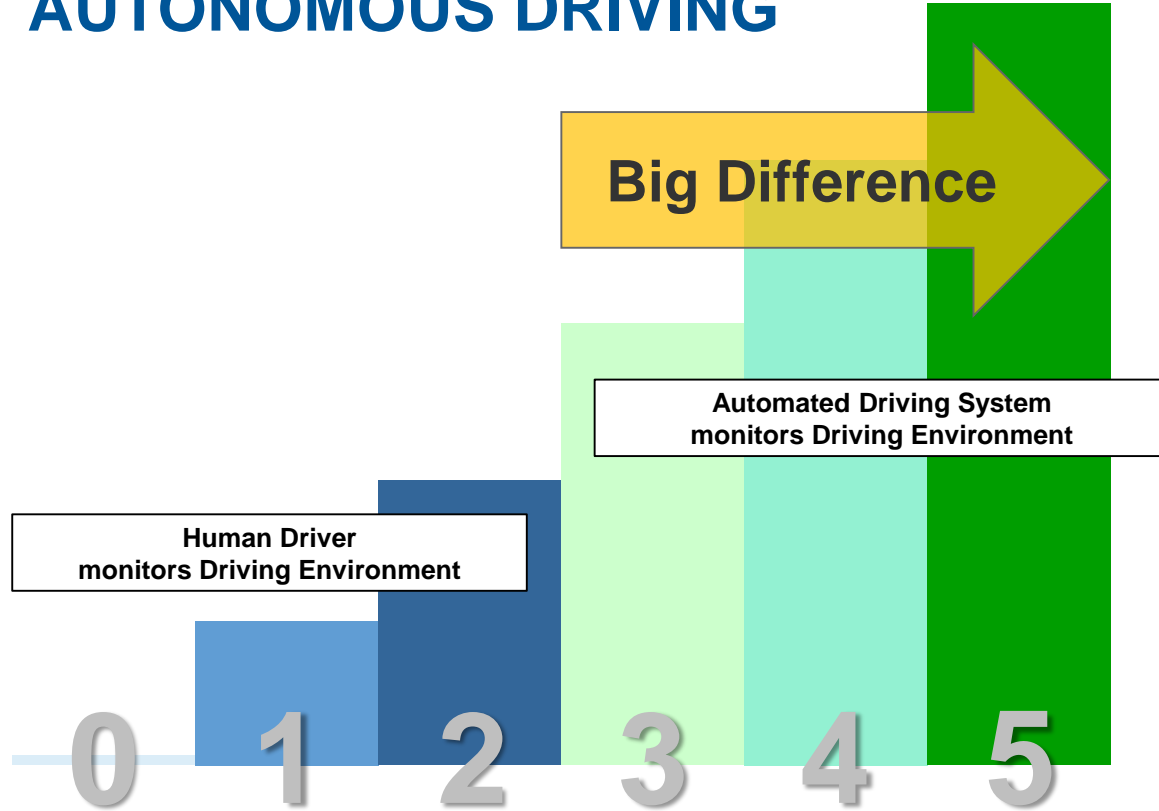


**Connectivity & Security**

**Complexity –  
Domain Integration**

**Life Cycles &  
Development Processes**

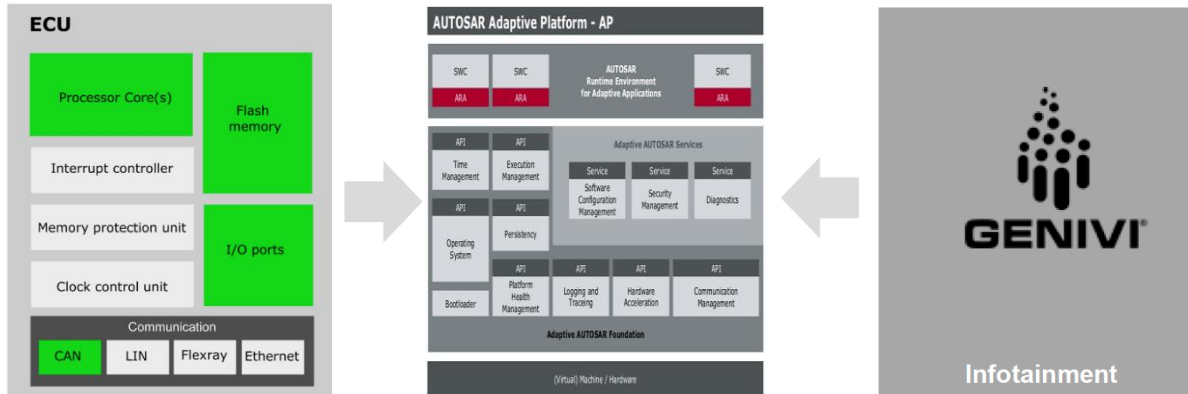
# LEVEL OF AUTONOMOUS DRIVING





Real time requirements

Safety relevance

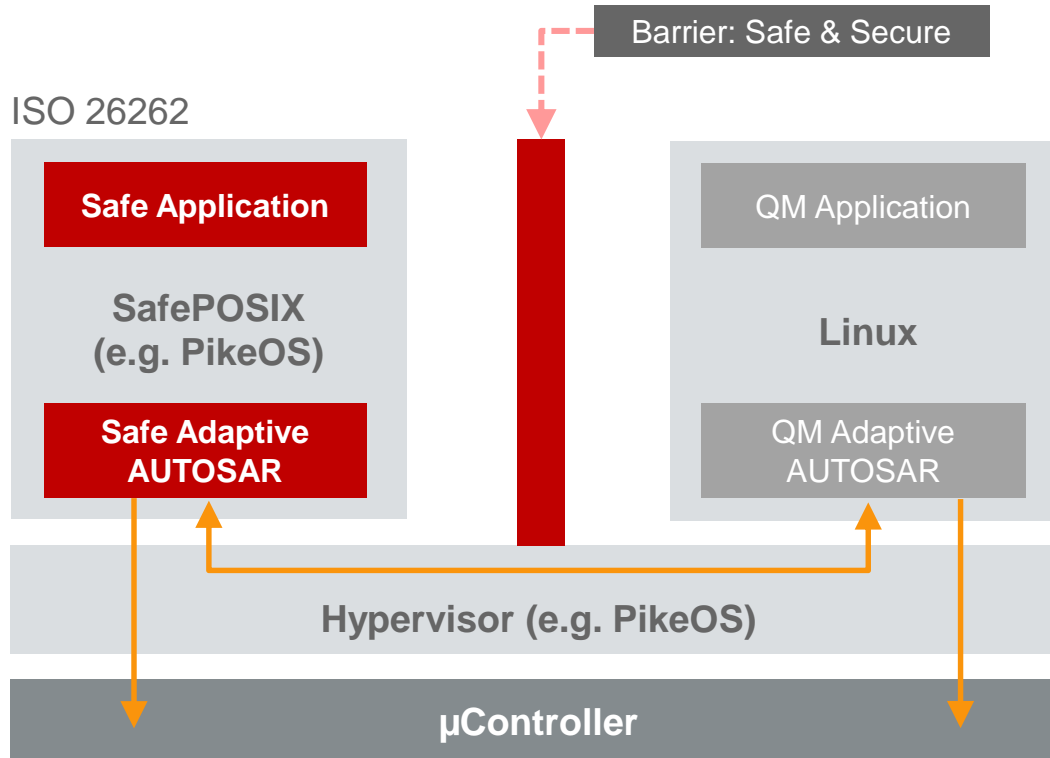


Security

Computing power

**AUTOSAR: “Another platform for different applications”**

# AUTOSAR ADAPTIVE – NEW STANDARD, NEW FEATURE



**Hypervisor  
combines  
Safety and Linux**



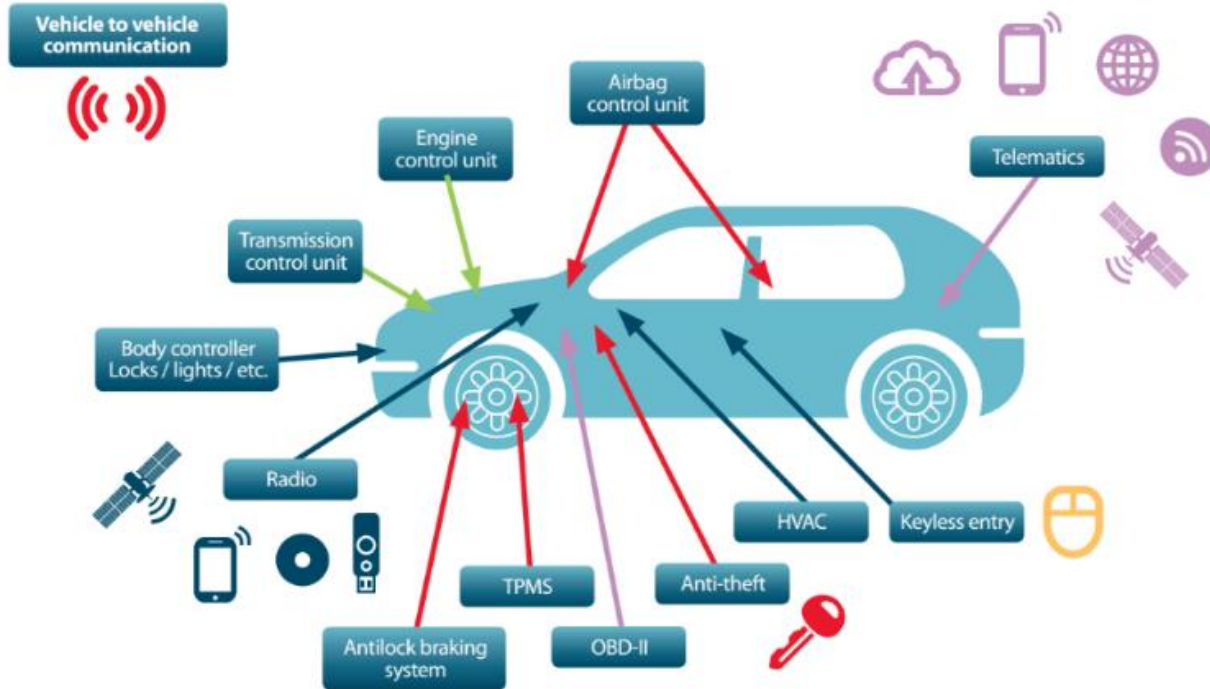
# What Security means

**CYBER CRIME CYBER C**  
**CYBER CRIME CYBER C**  
**CYBER CRIME CYBER C**

**Data Security – Privacy**

**Security for Safety**

# CONNECTED CAR – ATTACK SURFACE ELDORADO

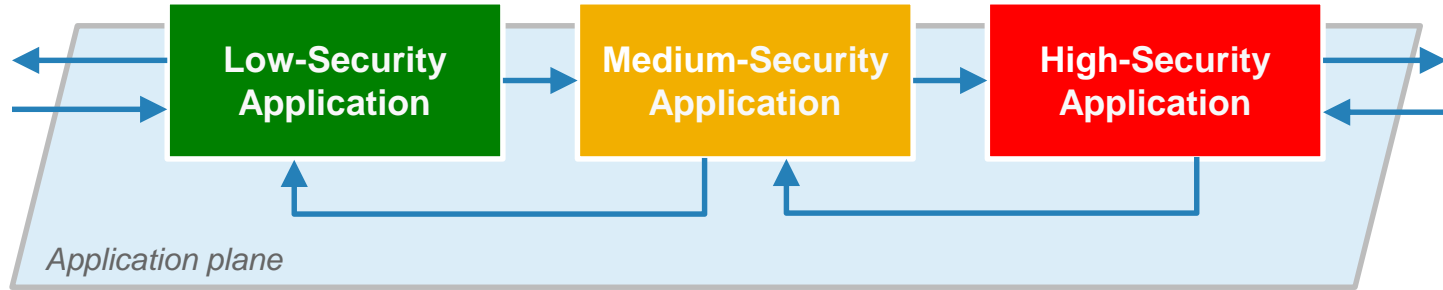


# OTHER PERSPECTIVE

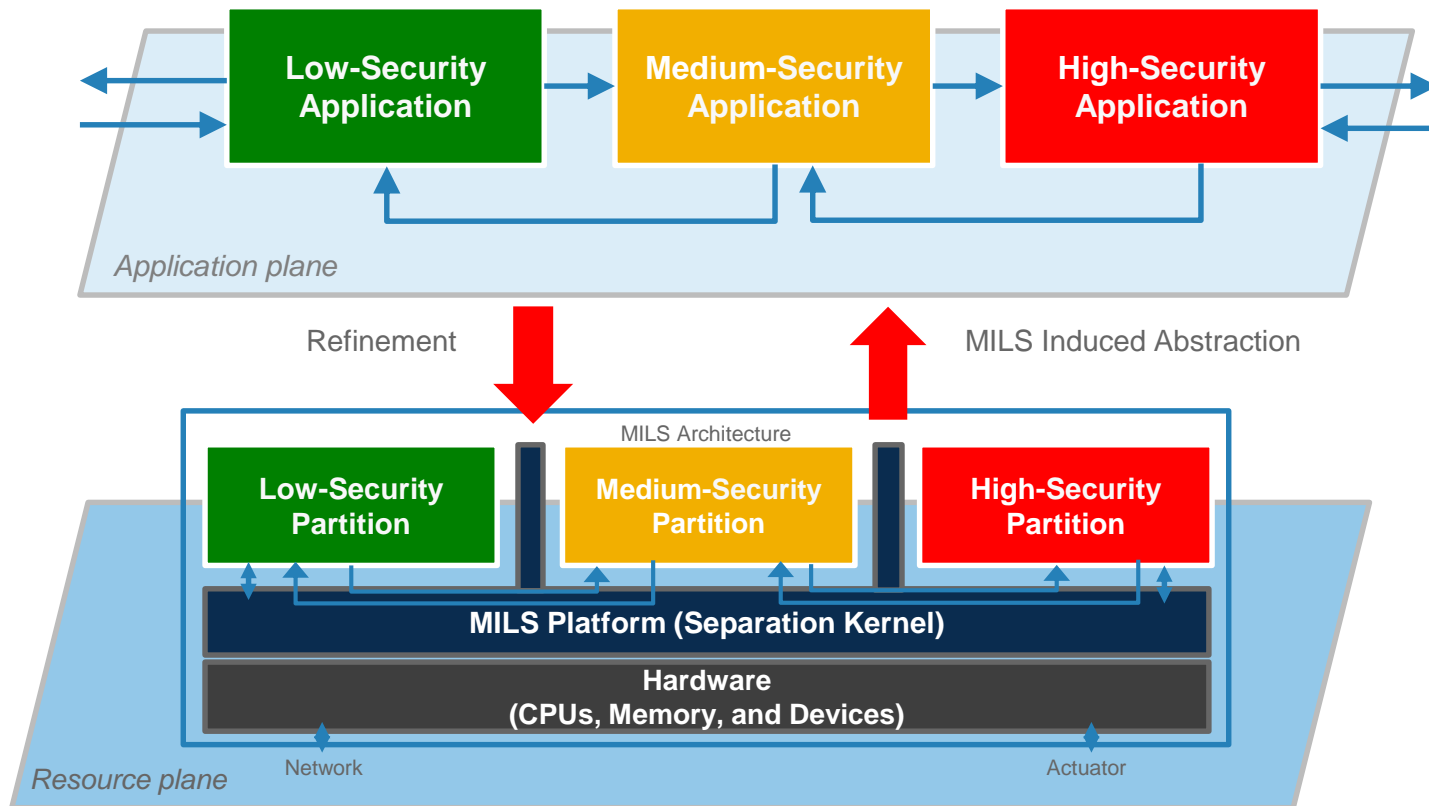
## LEARNING FROM IT SECURITY







**MILS** is a **high-assurance security architecture** that supports the **coexistence** of untrusted and trusted components, based on **verifiable separation mechanisms** and **controlled information flow**.



# Benefits

## MILS OS as Base for Future Automotive Platforms

Create Multi Domain Platform  
Supports New Mobility Services

Ensure strict Separation, Domain Integration  
Increase Data Privacy, Minimise Security Risks

Reduce Development Cost  
Minimize Risk for 3rd Party Components



Adaptive  
Autosar

Genivi /  
AGL

Other OEM  
Innovations

## Common Safety & Security Base

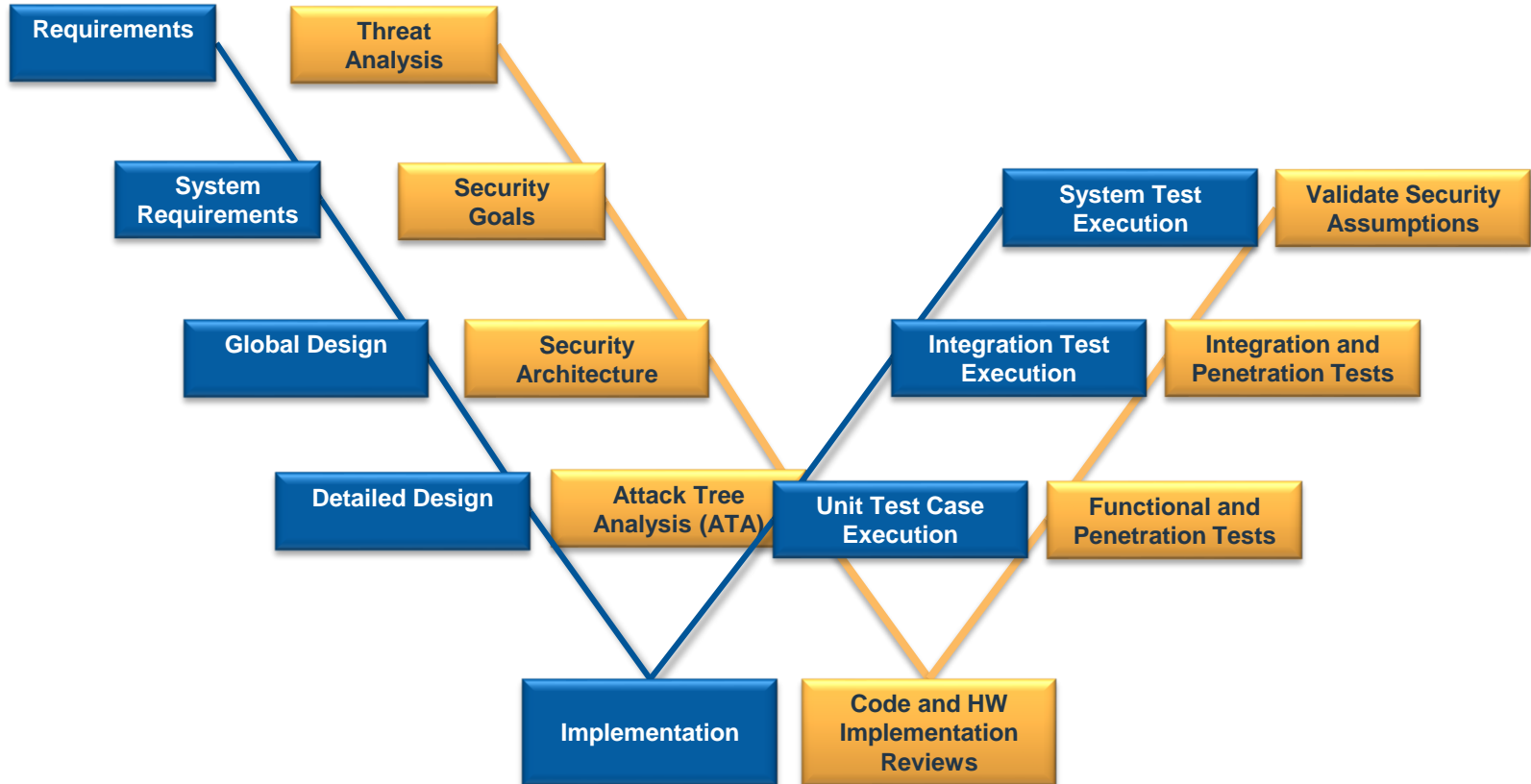
**ISO 26262**

**SAE J3101**

Hardware-Protected Security for  
Ground Vehicle Applications

**ISO/SAE 21434 -  
SAE J3061**

Cyber Security Guidebook  
for Cyber-Physical Vehicle Systems



**Secure Boot**

**Secure Update**

**Firewall**

**Intrusion Detection  
Systems**

**Controlled Communication  
Flow**

**MILS Separation Kernel**

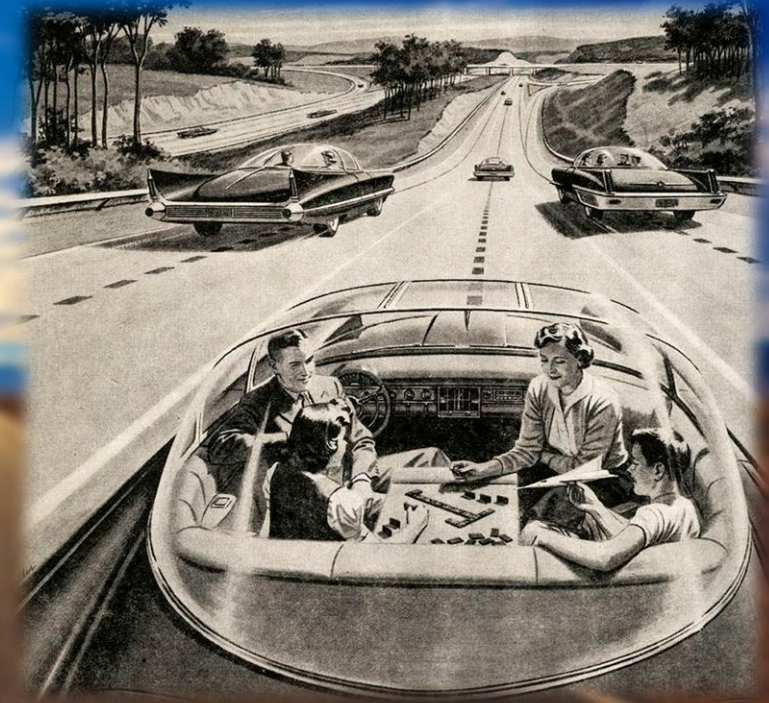


- **Understand the Standards and Recommendations**
  - **First Secure the Hardware**
  - **Then Secure the Software**
- System integration concept, i.e. architecture is the **most important Security MEASUREMENT**
- Ask if your software has:
- Monitoring
  - Assessment
  - Notifications
  - Remediations
  - Safe & Secure Software Life Cycle
  - Establish End-to-End Security



# Autonomous Driving

Let's make the  
Vision happen





# MASTER WITH US THE AUTONOMOUS DRIVING SAFETY & SECURITY CHALLENGES

**SYSGO**  
EMBEDDING INNOVATIONS

**EPT** 烽星科技

