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.

<table>
<thead>
<tr>
<th>PikeOS®</th>
<th>ELinOS</th>
<th>Board Support Packages</th>
<th>Certification Kits</th>
<th>Professional Services</th>
</tr>
</thead>
<tbody>
<tr>
<td>Separation Kernel based RTOS with integrated and certified virtualization technology (Hypervisor)</td>
<td>Industrial grade Linux Distribution for embedded systems with real-time extensions</td>
<td>Adaptation to the selected architecture, board specific initialization and drivers</td>
<td>Extensive collection of certification artefacts for all major generic and industry-specific standards</td>
<td>We make sure customers can optimize use our technology from prototyping to certification</td>
</tr>
</tbody>
</table>
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
AUTONOMOUS
WHY'S

Increase Safety (69%)
Road Capacity (65%)
Mobility, Stress (~50%)
Less Emission (31%)
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

Human Driver monitors Driving Environment

Automated Driving System monitors Driving Environment

Big Difference
SOFTWARE PLATFORMS

AUTOSAR: “Another platform for different applications”
AUTOSAR ADAPTIVE –
NEW STANDARD, NEW FEATURE

ISO 26262

Safe Application

SafePOSIX (e.g. PikeOS)

Safe Adaptive AUTOSAR

Barrier: Safe & Secure

QM Application

Linux

QM Adaptive AUTOSAR

Hypervisor (e.g. PikeOS)

μController

Hypervisor combines Safety and Linux
What Security means

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.
MILS Architectural Approach

Application plane

- Low-Security Application
- Medium-Security Application
- High-Security Application

Refinement

MILS Induced Abstraction

MILS Architecture

Low-Security Partition

Medium-Security Partition

High-Security Partition

MILS Platform (Separation Kernel)

Hardware (CPUs, Memory, and Devices)

Resource plane

Network

Actuator
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
COMMON: ASSURANCE VIA STANDARDS

Common Safety & Security Base

- ISO 26262
- SAE J3101: Hardware-Protected Security for Ground Vehicle Applications

Adaptive Autosar
Genivi / AGL
Other OEM Innovations
SAFETY & SECURITY SW LIFECYCLE

- Requirements
- System Requirements
- Global Design
- Detailed Design
- Threat Analysis
- Security Goals
- Security Architecture
- Attack Tree Analysis (ATA)
- Unit Test Case Execution
- Implementation
- System Test Execution
- Integration Test Execution
- Integration and Penetration Tests
- Validate Security Assumptions
- Functional and Penetration Tests
- Code and HW Implementation Reviews
- Security Goals
- System Test Execution
- Validate Security Assumptions
- Functional and Penetration Tests
- Code and HW Implementation Reviews
WHAT ELSE?

- Secure Boot
- Secure Update
- Firewall
- Intrusion Detection Systems
- Controlled Communication Flow
- MILS Separation Kernel
MAIN CONCLUSIONS

• 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