TRANSITIONING TO A SAFE AND SECURE ZONAL ARCHITECTURE

S32G Vehicle Network Processor as the Foundation
Automotive E/E Architecture Evolution Paths: Logical and Physical
Potential Automotive OEM Architecture Migration Paths → Logical + Physical

- Flat tunneling
- Hybrid zonalization
- Deep zone optimization
- Distributed computing

CARMAKER-E
CARMAKERS-A,B,C
CARMAKER-D
CARMAKER-F

Logical Path
Physical Path

Potential Automotive OEM Architecture Migration Paths → Logical + Physical

- Flat tunneling
- Hybrid zonalization
- Deep zone optimization
- Distributed computing

CARMAKER-E
CARMAKERS-A,B,C
CARMAKER-D
CARMAKER-F

Logical Path
Physical Path

PUBLIC
OVERVIEW

• We’re tasked with transitioning legacy to Zonal E/E Architecture
  • GuardKnox will assume the role of OEM engineering
• We’ll have a workshop with suppliers
  • NXP and Green Hills Software
APPROACH

• WHY ... ?
• WHAT ... ?
• WHERE ... ?
• HOW ... ?
• WHEN ... ?
WHY?
THE AUTOMOTIVE INDUSTRY IS IN THE MIDST OF A PARADIGM SHIFT

PROBLEMS & CHALLENGES

SCALABILITY WALL

• Too many ECUs
• Too much wiring
• Limited network configurations
• Coupled functionality

INDUSTRY LANDSCAPE

• New propulsion
• New consumer
• New competitors
• Upcoming regulation
ETHERNET BACKBONE - TOPOLOGY OPTIONS

PHYSICAL TOPOLOGY

LOGICAL TOPOLOGY

TREE TOPOLOGY - PHYSICAL LAYOUT

STAR TOPOLOGY - PHYSICAL LAYOUT

TREE TOPOLOGY - LOGICAL LAYOUT

STAR TOPOLOGY - LOGICAL LAYOUT
ZONAL ARCHITECTURE DEVICE CLASSES

VEHICLE SERVER
(general purpose computer)

ZONAL GATEWAY
(localized connectivity hub)
GOALS

01 END UP WITH A ZONAL ARCHITECTURE

02 REDUCE COSTS AS FAST AS POSSIBLE

03 BACKWARD AND FORWARD COMPATIBLE
WHAT?
WHICH DEVICE?

VEHICLE SERVER – ECU REDUCTION

• Transition to server(s)
• Network agnostic
• Agnostic to physical layout
• Cost reduction for any car
• Scales up / down
• Major impact on cost (engineering)

VS.

ZONAL GATEWAY – WIRING REDUCTION

• Introduce new gateway(s)
• Changes to backbone
• Depended on physical layout
• Cost reduction for wiring burdened car
• Unclear scaling
• Some impact on cost (material and labour)

MEETS OUR GOALS

WE’LL KEEP THAT IN MIND
## OBJECTIVES

### CONSOLIDATED PLATFORM
- Function = software package
- Stop ordering individual ECUs

### DE-FRAGMENT ECO-SYSTEM
- Runtime environments and versions
- Shorten development, certification and integration times

### FUTURE PROOF
- Single design fits many use cases
- Incremental functionality development
COMMONALITY

- Powertrain = $\mu$C + Interfaces
- Cockpit = $\mu$P + $\mu$C + Interfaces + GPU
- Connectivity = $\mu$P + Interfaces + Wireless
- Body = $\mu$P + $\mu$C + Interfaces
- Autonomy / ADAS = $\mu$P + $\mu$C + Interfaces + Vision / GPU
- Battery = $\mu$C + Interfaces + PLC / Wireless
- Gateway = $\mu$P + $\mu$C + Interfaces
- Legacy = $\mu$P / $\mu$C + Interfaces + ASICs

SERVER = $\mu$P + $\mu$C + Interfaces
WHERE?
CONSTRANTS

- Replace an existing ECU
- Biggest network outreach
- Place to scale

“CENTRAL” EXISTING ECU → SERVER PLATFORM
GATEWAY ARCHITECTURE

BLOCK DIAGRAM

NETWORK TOPOLOGY (STAR-ISH)
GATEWAY TO ZONAL

18 | www.guardknox.com
DOMAIN TO ZONAL

GDC

GDC + SERVER

[Diagram showing the flow from GDC to GDC + Server]
HOW?
**VEHICLE SERVER “TEMPLATE”**

- Consolidated
  - Single SoC
  - Software modules
- Mixed criticality
  - Safety
  - Security
- Scalable
  - Clustering
  - Device family
  - Runtime environments
- Secure (inclusive safety)
  - Defense in depth
  - Logical / physical isolation
REQUIREMENTS

01 Micro-processor (application)
02 Micro-controller (real-time)
03 Up to ASIL-D (applications are unknown)
04 All automotive interfaces (legacy and Ethernet)
05 Multiple runtime environments (hypervisor / processors)
06 Scalable platform (hardware family variants)
07 Strong isolation (safety and security)
08 NO APPLICATION RE-DEVELOPMENT!
S32G is a New Type of Automotive Processor:
Vehicle Network Processor

**PROCESSING**
- Lockstep Microcontrollers
- Cluster Lockstep Microprocessors
- Automotive Networks Acceleration
- Ethernet Packet Acceleration

**NETWORKING**
- 20 x CAN/CAN FD Interfaces
- LIN and FlexRay™ Interfaces
- 4 x Gigabit Ethernet Interfaces
- PCI Express Gen 3 Interfaces

**SAFETY & SECURITY**
- ASIL D Functional Safety Support
- Advanced Hardware Security Engine

**APPLICATIONS**
- Service-oriented Gateway
- Domain Controller
- ADAS/AD Safety Controller
- Vehicle Compute / Zonal Gateways

www.nxp.com/S32G
S32G Processor Supports Vehicle Architecture Transformation

**CONNECTIVITY**
- **INFOTAINMENT & IN-VEHICLE EXPERIENCE**
- **ADAS & HIGHLY AUTOMATED DRIVING**
- **SERVICE ORIENTED GATEWAY**
- **POWERTRAIN & VEHICLE DYNAMICS**
- **BODY & COMFORT**

**LEGACY APPROACH | FLAT**
- UNFIT TO FUTURE MOBILITY – SECURITY AND SCALABILITY ISSUES
  - Low bandwidth, one MCU per application

**LOGICAL RESTRUCTURE | DOMAINS**
- ENABLING SCALABLE GROWTH, CONSOLIDATION AND NEW FEATURES LIKE AUTONOMOUS VEHICLE
  - High bandwidth network
  - Gateway key to communication between domains
  - Domain Controllers for local networking and ECU consolidation

**PHYSICAL RESTRUCTURE | ZONES**
- REDUCING WIRING COMPLEXITY AND ENABLING THE USER-DEFINED CAR
  - Domains virtualized by SW – enabling high flexibility
  - Easy enable/disable or update functions
S32G274A: ASIL D Vehicle Network Processor

On-the-Fly
Secure External
Flash Memory

Functional
Safety Design

Embedded
Hardware
Security with
PKI Support

MCUs for real-
time processing

MPUs for apps
and services

Automotive
Networks
(CAN/LIN/FlexRay)
Hardware
Acceleration

Automotive
Gigabit Ethernet
Hardware
Acceleration

System Peripherals and Interfaces
including 2x2 PCI 3.0

System Peripherals and Interfaces
including 2x2 PCI 3.0
S32G Scalable Family Applications*

**Advanced Service-oriented Gateway, Connected Gateway, AD Domain Controller**

Maximum processing performance for services, domain control and communications stacks  ♦ Maximum ASIL D performance

**Basic Service-oriented Gateway, Domain Controller**

Maximum real-time performance ♦ Application processing for services and domain control

**Ethernet Gateway, Management Controller**

Application processing for management and control ♦ Some real-time processing for automotive networking

**Low/Mid-range Gateway, Zonal I/O Controller, Safety Controller**

Maximum real-time performance for automotive networking and safety control ♦ No applications processing

*These applications are only for guidance and can vary based on customer requirements.
Accelerating Transformation Across the Automotive Ecosystem

**Carmakers**
- Proof of concept
- Benchmarking
- Vehicle data insights
- New services deployment

**Application Developers**
- Innovation platform
- Software development
- Test and validation
- Demo showcase

**Cloud & Service Providers**
- Symbiotic compute
- Over-the-Air (OTA) updates
- Machine learning deployment
- Edge service deployment

**NXP S32G Reference Design Board Accelerates Development**
Mixed-Criticality as an Enabler

- The main driver is the application landscape
  - Domain controllers & vehicle computers
  - ADAS/AD Applications
  - Gateways
  - Modular software deployment
  - ‘App-store’ like software distribution

- Heterogeneous computing platforms to the rescue
  - Require vast middleware packages
  - Enable rich connectivity functions

- Mixed criticality on a single platform is the key
A failure in an element is caused by a fault

Faults can have diverse root causes
- Hardware faults – bit flips, erratas, etc.
- Software faults – bugs
- Malicious attacks

FFI prevents failures from propagating (cascading)
- Relevant for the safety functions of an ECU

FFI is critical for separating mixed-criticality systems
- Prevents failures to cascade from “lower” ASIL to “higher” ASIL
- Prevents failures to cascade within the same ASIL domain
Mixed-Criticality in Action

- A pre-certified secure microkernel
  - Minimal codebase, low footprint, efficient hardware resource usage
  - Trusted secure base for separation
- Least privilege model provides “containerization”
  - Additionally enhanced by virtualization capabilities

Green Hills Software INTEGRITY RTOS

Core 1  •••  Core n  •••  NXP S32G  •••  Packet Forwarding Engine  •••  Peripherals
**SOFTWARE STACK LAYOUT**

- **App domain**
  - Quad A53
  - Split/lock
  - RTOS
  - Hypervisor

- **RT domain**
  - Triple M7
  - Lockstep
  - RTOS
  - Bare metal

- **Accelerators**
  - Network
  - Security

---

**SYSTEM ARCHITECTURE**

1. **App domain**
   - Arm Cortex-A53 (split/lock)
   - Green Hills Software INTEGRITY RTOS (Separation Kernel)
   - Hosted OS
   - Multivisor VMM (Hypervisor)

2. **RT domain**
   - Arm Cortex-M7 (Lockstep)
   - Safety RTOS
   - RTOS

3. **Interfaces and accelerators**
   - Arm Cortex-M7 (Lockstep)
   - Arm Cortex-M7 (Lockstep)
HARDWARE ENFORCED ISOLATION

- App domain → MMU
- RT domain → MPU
- Interconnect → XRDC
CONSOLIDATION: USE CASE

- Runtime
  - AUTOSAR Classic
  - AUTOSAR Adaptive
  - Linux
  - Bare metal
- Vendors
  - AUTOSAR Classic
  - ECU suppliers
- Criticalities
  - ASIL-D
  - ASIL-B
  - QM
  - Unspecified

Legacy ECUs

- AUTOSAR Classic A (ASIL-D)
- AUTOSAR Classic A (ASIL-B)
- AUTOSAR Classic B (ASIL-B)
- Linux + AUTOSAR Adaptive (QM)
- Bare metal (?)
USE CASE IMPLEMENTATION A

- **App domain**
  - Quad A53
  - Split/lock
  - RTOS
  - Hypervisor
- **RT domain**
  - Triple M7
  - Lockstep
  - RTOS
  - Bare metal
- **Accelerators**
  - Network
  - Security

![Diagram showing USE CASE IMPLEMENTATION A](image-url)
USE CASE IMPLEMENTATION B

- **App domain**
  - Dual A53
  - Split/lock
  - RTOS
  - Hypervisor

- **RT domain**
  - Single M7
  - Lockstep
  - RTOS

- **Accelerators**
  - Network
  - Security

---

**Diagram:**

- App domain
  - Dual A53
  - Split/lock
  - RTOS
  - Hypervisor

- RT domain
  - Single M7
  - Lockstep
  - RTOS

- Accelerators
  - Network
  - Security

---

- **Autosar Classic (Vendor A)**
- **Autosar Adaptive**
- **Autosar Classic (Vendor B)**
- **Multivisor VMM (Hypervisor)**

- **Green Hills Software INTEGRITY RTOS**
  - (Separation Kernel)

- **Arm Cortex-A53**
  - (Split/lock)

- **Arm Cortex-M7**
  - (Lockstep)

- **Interfaces and accelerators**
ZONAL GATEWAY

• Re-use gateway + server design
• Optimize case by case
UNIFORMITY

• Maximize software re-use
  • MCAL / BSP
  • Applications
  • Guest OS / middleware / eco-system

• Hardware scaling up / down
  • Pin compatibility
  • Vendor roadmap
  • Product / chip family and variants

• Interchangeable parts
  • May not need to maintain old ECUs
  • May not need to stock up parts for over a decade
  • Used car factory options “retrofitting”

• Vendor complementary peripherals
  • Design optimized PMIC, Ethernet switches, transceivers...
CHALLENGES AND PITFALLS

• Cost reduction
  • Across entire E/E
  • Vehicle lifecycle

• Not a traditional supplier engagement
  • Requires expertise - no general solution
  • Can’t spec-out “make me have zonal”

• DMIPS performance rating
  • Accelerators and offloaders are left out
  • Today mostly a compiler optimizer benchmark
WHEN?
PARTNER MAPPING

GUARDKNOX VEHICLE SERVER REFERENCE DESIGN

SAFETY- AND SECURITY-CRITICAL APPS

- Applications
- Safe OS 1 (e.g. AUTOSAR Classic/Adaptive)
- GuardKnox Secure Comm.
- GuardKnox Security Monitor
- GuardKnox Lockdown Core
- GuardKnox Crypto
- GuardKnox Comm. Agent
- Third Party Applications and Services

NON-REAL-TIME APPS

- Applications
- GuardKnox Cloud Connectivity
- GuardKnox Container
- Third Party Applications and Services
- Safe OS 2
- Linux
- INTEGRITY Multivisor
- INTEGRITY Multivisor
- INTEGRITY Multivisor

Green Hills INTEGRITY RTOS

NXP S32G Vehicle Network Processor
THANK YOU

Idan Nadav
Idan@guardknox.com
http://www.guardknox.com

Nikola Velinov
Nvelinov@ghs.com
http://www.ghs.com

Brian Carlson
Brian.carlslon@nxp.com
http://www.nxp.com