Introduction to Requirement Management for Safety-Critical Embedded Vehicle Systems

SARE-väst, May 2013

Urban Ingelsson
Safety-Critical Systems Competence Center
urban.ingelsson@semcon.com
What is functional safety?

- Absence of unreasonable risk due to hazards caused by malfunctioning behavior of E/E systems
- Brakes, steering, ...
- Electronics and software
- ... could cause an accident
- "certifiably" safe embedded systems in automotive context
  - ISO 26262 "Functional Safety – Road Vehicles"
ISO 26262

- Structured way of working
- Scope
- Specification and management of requirements
- Hazard analysis and risk assessment
- Automotive Safety Integrity Levels – ASIL

![ASIL Levels Diagram]

"Effort"  Criticality

ASIL D
ASIL C
ASIL B
ASIL A
Quality Management (QM)
Case study
Windshield Wiper

Washer Liquid Spray Activate
Wiper Activate
Wiper Enable
Wiper Angle

Windshield controller

Washer Liquid Spray Enable

Is it a safety-related function?
The driver’s view might be obscured

Failure mode
Contineous spray of washer liquid

Driving situation
High speed, curvy road, medium traffic

Exposure
High

Controllability
Medium

Severity
High

Safety goal
A malfunction shall not lead to the driver’s view being obscured
Introduction to Requirement Management for Safety-Critical Embedded Vehicle Systems

May 2013

HAZOP, etc.

Exposure
Controlability
Severity

FTA, etc.

Design space exploration
Compare design patterns

Quality attributes, notation, etc.
ASIL C? It takes much effort!
Reduce effort by requirement decomposition!

• A divide-and-conquer approach
  – Encourages use of safe architectures
  – 2 independent modules
    • “freedom from interference”

lower ASIL --- typically less effort
**FSR1**
The washer liquid spray shall not be enabled for >5s

**FSR2**
The washer liquid spray shall not be enabled for >1s if the wiper is inoperational

**FSR3**
The washer liquid spray controller shall disable the washer liquid spray, if the windshield wiper angle is constant for >1s

**FSR4**
The wiper controller shall disable the washer liquid spray, if the washer liquid spray is enabled for >5s
Quality attributes for requirements

Each requirement
• Uniquely identified
• Allocated in the design
• Unambiguous
• Comprehensible
• Atomic
• Internally consistent
• Feasible
• Verifiable
• High ASIL: spec. in semi-formal notation
• Traceable
  – Up and down the hierarchy
  – Verification activities, operating modes and system states

The set of requirements
• Organized in a hierarchy
• Complete
• Grouped
• Consistent
• Maintainable
• Free from duplicated information
SG1: A malfunction shall not lead to the driver’s view being obscured

FSR3: The washer liquid spray controller shall disable the washer liquid spray, if the windshield wiper angle is constant for >1s

FSR4: The wiper controller shall disable the washer liquid spray, if the washer liquid spray is enabled for >5s

TSR42: Counter1 shall be reset within 20ms when Comparator3 indicates that PreviousAnglePWM ≠ anglePWM

SWSR50: Control loop L1 shall reset Counter1 if Comparator3.output == false

HWSR71: Register anglePWM shall connect on the same bus as inputA of Comparator3
Conclusion

• The impact of ISO 26262
  – Requirement-heavy
  – ASIL
  – Quality attributes, traceability and semi-formal notation

• Effort

• Architecture
Introduction to Requirement Management for Safety-Critical Embedded Vehicle Systems

SARE-väst, May 2013

Urban Ingelsson
Safety-Critical Systems Competence Center
urban.ingelsson@semcon.com