Software development for safety-related automotive systems – the MISRA guidelines and ISO 26262

Dr David Ward
General Manager
Functional Safety

© MIRA Ltd 2010

MIRA

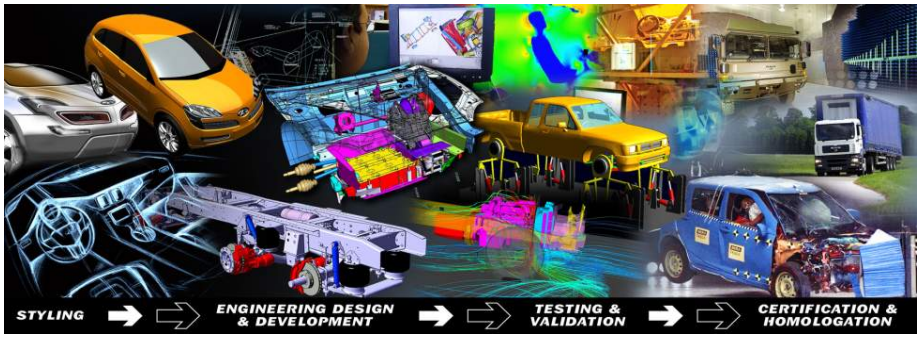
Agenda

- Motivations and challenges for system safety in the automotive industry
- What is the automotive industry doing?
- What are some of the future directions?
- How might these relate to other sectors?

MIRA

© MIRA Ltd 2010. All rights reserved.

MIRA delivers world class and independent vehicle engineering consultancy to the global automotive and transport industries



- Diverse global customer base from automotive, defence, aerospace and rail sectors
- Full vehicle systems design, test and integration engineering expertise — a "one-stop-shop"
- Discrete system engineering projects through to turnkey vehicle development programmes
- Advanced concept through to post-production support
- Unrivalled experience applied through a flexible, high-quality approach utilizing the latest tools and techniques
- Providers of advanced research and development, cutting edge technology to leaders in industry

MIRA

The MISRA project

- Started in 1990
- Mission: "to provide assistance to the automotive industry in the creation and application of safe and reliable software in vehicle systems"
- The original project was part of the UK Government's "SafeIT" programme
- Now self-supported

MISRA®

MIRA

© MIRA Ltd 2010. All rights reserved.

MISRA interests

- MISRA aims to
  - ✓ Promote best practice in automotive safety-related systems engineering
  - ✓ Develop guidance in specific technical areas in an "engineer-friendly" manner
- MISRA does not
  - ✗ Run certification schemes
  - ✗ Promote or endorse specific products

MIRA

MISRA activities

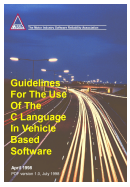
- General engineering issues
  - MISRA Guidelines (1994)
  - Software readiness for production
  - MISRA Safety Analysis
- Language-specific issues
  - MISRA C
  - MISRA C++
  - MISRA AC family
  - MISRA Languages (planned)

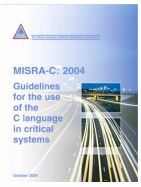
MIRA

© MIRA Ltd 2010. All rights reserved.

Key MISRA publications

- November 1994: *Development guidelines for vehicle based software* (The MISRA Guidelines)
- April 1998: *Guidelines for the use of the C language in vehicle based software* (MISRA C)
- October 2004: *MISRA-C:2004 – Guidelines for the use of the C language in critical systems* (MISRA C2)
- November 2007: *Guidelines for safety analysis of vehicle based programmable systems* (MISRA SA)
- November 2007 onwards: MISRA AC family (model-based development/ autocode)



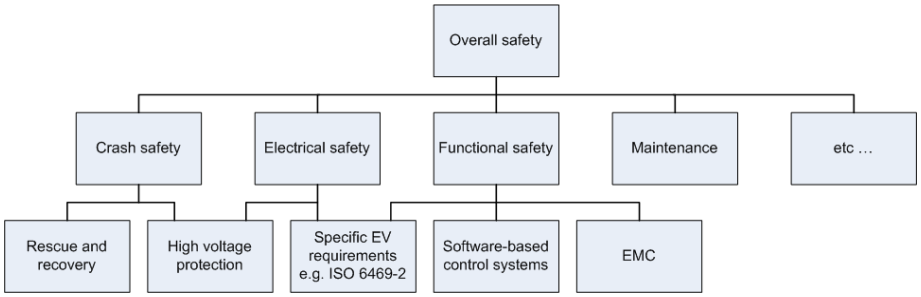


Automotive system safety

- Safety has long been an important part of automotive engineering
  - But traditionally focused on specific areas e.g. in crashworthiness active and passive safety
- The increased technical sophistication of vehicles means a system-led approach to their safety is needed
  - Particularly, but not limited to, hybrid and electric vehicles

© MIRA Ltd 2010. All rights reserved.

Hybrid vehicle safety

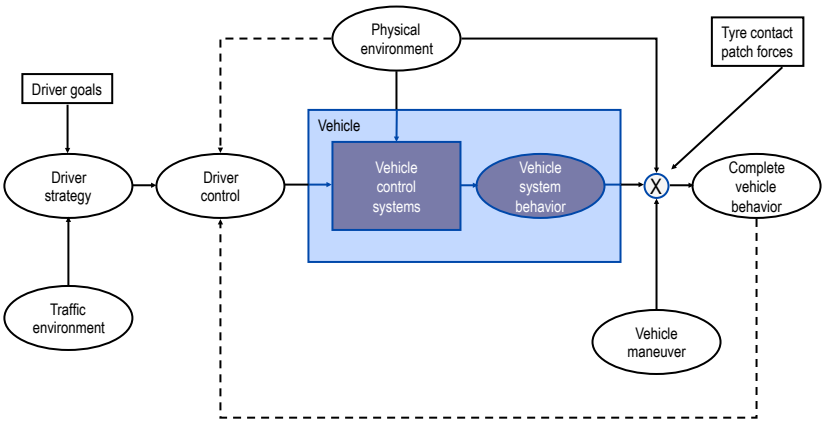


Unique automotive safety issues

- Mass-market consumer product
  - We all have a view!
  - Any perceived issues can lead to widespread adverse publicity
- Driver is part of control loop but receives little formal training in operating safety-related systems
- Long product lifetimes with maintenance difficult to assure outside warranty

© MIRA Ltd 2010. All rights reserved.

"Driver in the loop" model



Specific automotive challenges

- Distributed control systems with high dependence on complex software
- Hybrid and electric vehicles – new systems with new potential failure modes
- "Drive by wire" systems
  - Working assumption that "off" is a safe state i.e. it is acceptable for systems to fail safe

© MIRA Ltd 2010. All rights reserved.

The future

- Further integration, higher feature content
- Drive-by-wire systems that must be fault-tolerant
  - Brakes, steering
- Vehicle-to-X communications
  - Co-operative driving
  - Input to vehicle objectives from outside e.g. emissions control in sensitive areas

MIRA

The future continued

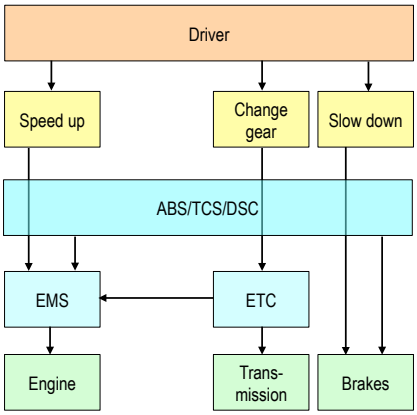
- Autonomy e.g. unmanned ground vehicles (UGVs)
  - Vienna Convention: "Every vehicle must have a driver"
  - However … autonomy has many applications in defense, aerospace
    - May be based on technology from mass-market products

MIRA

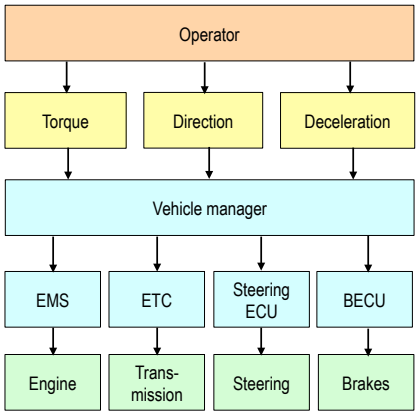
© MIRA Ltd 2010. All rights reserved.

Distributed control systems

Traditional vehicle



UGVs



Automotive system safety standards

- Early 1990s – work on functional safety in IEC SC 65A
  - Generic aspects of functional safety
  - Software
- 1994 MISRA *Development Guidelines for Vehicle Based Software*
- 1998 – 2000 IEC 61508 published
  - Now in 7 parts

© MIRA Ltd 2010. All rights reserved.

Automotive system safety standards

- 2004 German and French national initiatives
- November 2005 Official start of work on ISO 26262 *Road vehicles — Functional safety* at international level
- November 2007 MISRA *Guidelines for Safety Analysis of Vehicle Based Programmable Systems* (MISRA SA)
- July 2009 ISO 26262 published as DIS (draft international standard)
- Mid-2011 (latest) – full international standard

MIRA

IEC 61508

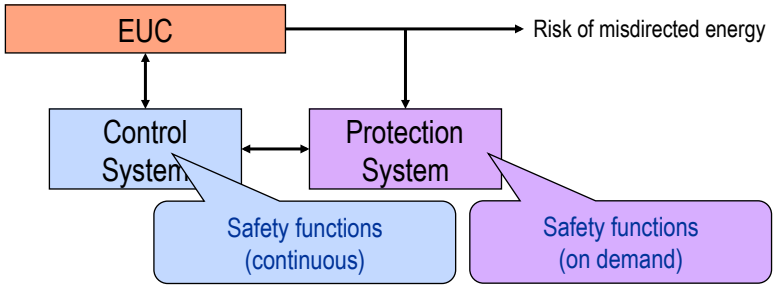
- *Functional safety of electrical, electronic and programmable electronic safety-related systems*
- The benchmark standard for developing and validating safety-related electronic systems
- Main principles are
  - Identify system risk and required risk mitigation (expressed as a Safety Integrity Level, SIL)
  - Perform the development and validation with a rigor matching the SIL
  - Demonstrate that the required risk reduction has been achieved
- Note that the risk reduction is **usually** achieved through a **separate** protection system or safety function

MIRA

© MIRA Ltd 2010. All rights reserved.

Basis of IEC 61508

- There is Equipment Under Control (EUC) which poses a threat to its environment



- Safety functions are performed by E/E/PE systems
- Steps need to be taken to understand the risks involved and reduce them to an acceptable level

Some issues with applying IEC 61508 to automotive

- Developed for low-volume not mass-market products
- Methods for risk analysis are informative and industry interpretation is always needed
- Subcontracting of work not addressed
- Human factors issues only briefly addressed
  - Does not address the “driver in the loop”
- Does not reflect state-of-the art automotive development processes e.g. use of embedded systems and model-based development

© MIRA Ltd 2010. All rights reserved.

MISRA Safety Analysis

- *Guidelines for safety analysis of vehicle based programmable systems*
- Provides guidance on safety management
  - Useful for establishing processes e.g. in accordance with IEC 61508 or ISO 26262
- Provides process for automotive hazard and risk analysis
  - Explains this from "first principles"
- Risk graph for hazard classification
  - Permits adaptation or calibration for different application requirements e.g. UGVs
  - Takes account of designated safety systems

MIRA

ISO 26262

- *Road vehicles – Functional safety*
- A functional safety standard specifically for passenger cars
  - Claims to be "the" automotive version of IEC 61508
- Timetable
  - DIS (first public version) July 2009
  - FDIS (second public version) February 2011*
  - Full standard July 2011*
- Excluded from scope
  - Trucks and buses
  - Specialist adaptations of cars

* Guideline dates

MIRA

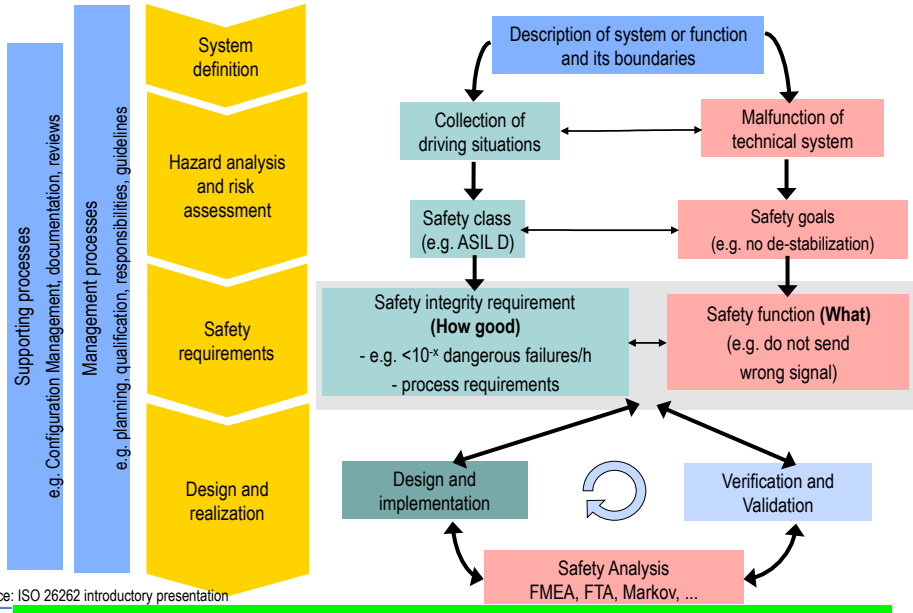
© MIRA Ltd 2010. All rights reserved.

Objectives of ISO 26262

- Maintain "comparability" with IEC 61508 for product liability reasons
- Adapt the safety lifecycle to the typical automotive development and operation phases
- Include requirements for relationships between manufacturers and suppliers, and for distributed development processes
- Adapt the hazard analysis and risk assessment for typical automotive use cases
- Allow for application of typical automotive validation tests
  - Hardware-in-the-loop, whole vehicle simulation environments, fleet tests and user-oriented tests

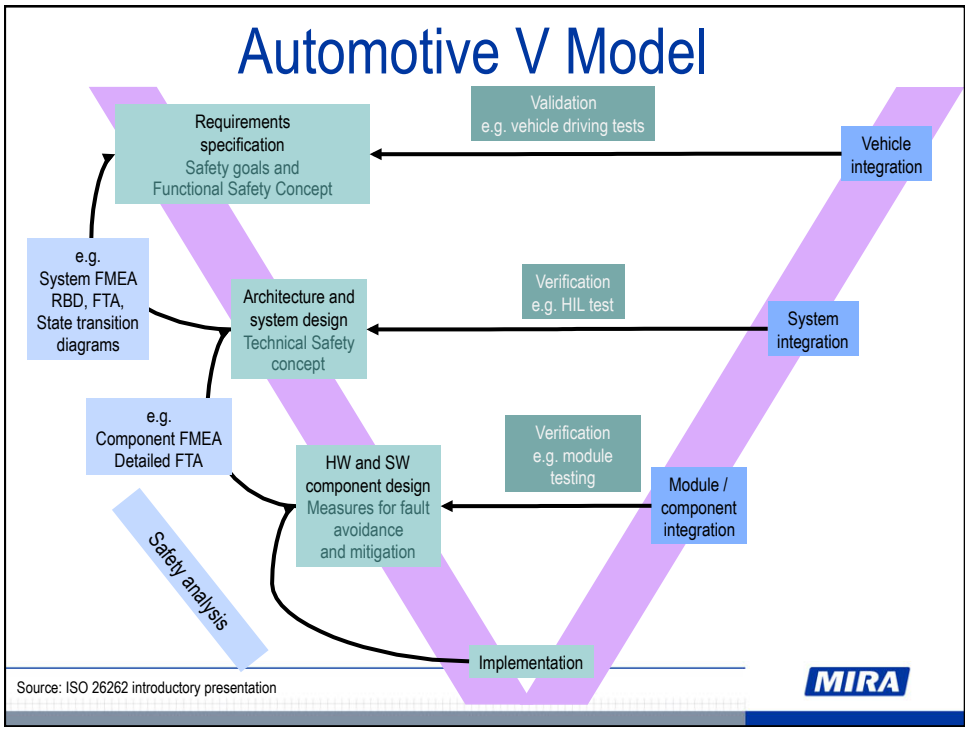
MIRA

Overview of an automotive functional safety process



Source: ISO 26262 introductory presentation

© MIRA Ltd 2010. All rights reserved.



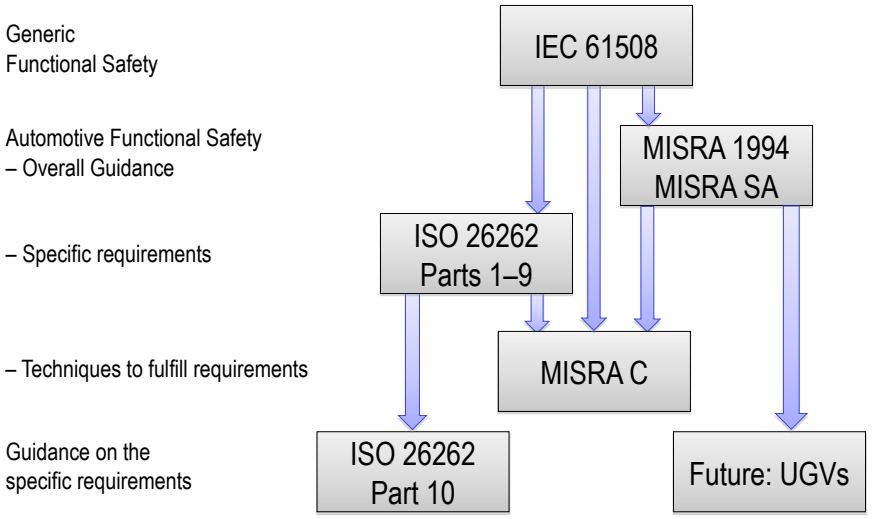
Some issues with ISO 26262

- ISO ASILs do not align with IEC SILs
  - ⇒ Difficult to "read across" components between different sectors
    - e.g. electric motor controller and battery management may be re-used in different applications
- No provision for emerging technology e.g.
  - Vehicle-to-X communication
  - Autonomy
  - Some systems in hybrid/electric vehicles more like the safety/protection systems of IEC 61508

MIRA

© MIRA Ltd 2010. All rights reserved.

Relationships between standards



So what about software?

- So far this presentation has (intentionally) focused on system approaches to system safety
  - A key strength of IEC 61508 and ISO 26262 is that design for safety is system-led
- Top-level safety requirements lead to requirements for system, hardware and software development
  - Development lifecycle
  - Specific requirements for process and product
  - Specific techniques (IEC) or methods (ISO)

© MIRA Ltd 2010. All rights reserved.

So where does MISRA C fit?

- Coding guidelines and subsets are required by many safety-related standards
  - Not only for C
- C is popular for embedded systems because
  - It is specified in an International Standard
  - It is widely implemented
  - Compiles into efficient code
  - It provides access to low-level machine features
- Its drawbacks include
  - Many aspects of program behavior not specified
  - Implementations vary widely
  - It provides access to low-level machine features
- MISRA C aims to reduce the uncertainties associated with these drawbacks

MIRA

MISRA C history

- First ISO C standard, “C90”, published in 1990 with corrections and amendments in 1995 and 1996
- First version of MISRA C published in 1998
- Second version published in 2004 with Technical Corrigendum in 2007
  - More specific and definitive guidance
  - Based on C90 as support for C99 by embedded compiler vendors was limited at the time
- Originally intended for automotive use but has become widely accepted in many industries

MIRA

© MIRA Ltd 2010. All rights reserved.

In conclusion

- The automotive industry has some specific challenges in safety-related systems and their software, but many of the general principles are the same
- MISRA C is a good example of how guidance developed for an automotive need has benefited other sectors
- Going forward we look forward to ongoing co-operation

MIRA

For further details

- David Ward
  - + 44 24 7635 5430
  - david (dot) ward (at) mira (dot) co (dot) uk
  - www.mira.co.uk
- MISRA information
  - www.misra.org.uk

MIRA

© MIRA Ltd 2010. All rights reserved.