Developments in ISO 26262

Dr David Ward – Global Head of Functional Safety

HORIBA MIRA Ltd

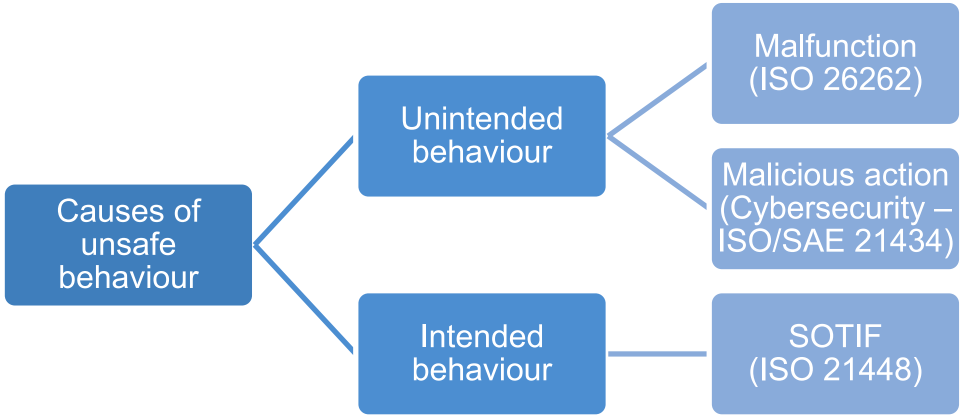
What is ISO 26262?

- ISO 26262:2018 Road vehicles – Functional safety

- The go-to standard for developing safety-related electrical / electronic systems in road vehicles

- Focusses on hazards caused by malfunctioning behaviour of electrical / electronic systems (including their interactions)

- However product safety must consider wider causes of unsafe behaviour



Key principles in ISO 26262

- Root causes of malfunctions are random hardware faults or systematic defects
- Product design needs to be robust against
  - Reasonably foreseeable causes of failure
  - Failures that can still occur at runtime
- The required robustness is specified in safety requirements and their associated ASIL values
- Architectural design is key to achieving robustness
  - Architectural properties include “freedom from interference” and “independence”
    - Separation of safety-related vs non-safety-related functionality
    - Separation of safety-related functionality with differing ASIL values (so-called “mixed criticality”)

Current status of ISO 26262

- Industry has nearly 20 years' experience developing and implementing the standard
- Principles are well-established and widely accepted
- Variances can still be seen in understanding and application e.g.
  - The term "ASIL" is well recognized but also too readily used without proper context
  - "Tick box" mentalities in evidence despite the standard being a process framework that specifies "what" we need to do but not necessarily the "how"
- Work just starting on Edition 3 with likely publication Q4/2027 (subject to change)

What are some of the challenges?

- ISO 26262 originally conceived against backdrop of “commodity” systems
  - The concept of the “item” e.g. braking, steering
- Significant changes in vehicle architectures culminating in zonal or centralized architectures
  - E.g. the “software defined vehicle”
- So what is the “item” now?
  - How do we scope safety activities?
  - How do we demonstrate freedom from interference etc. in the implementation?

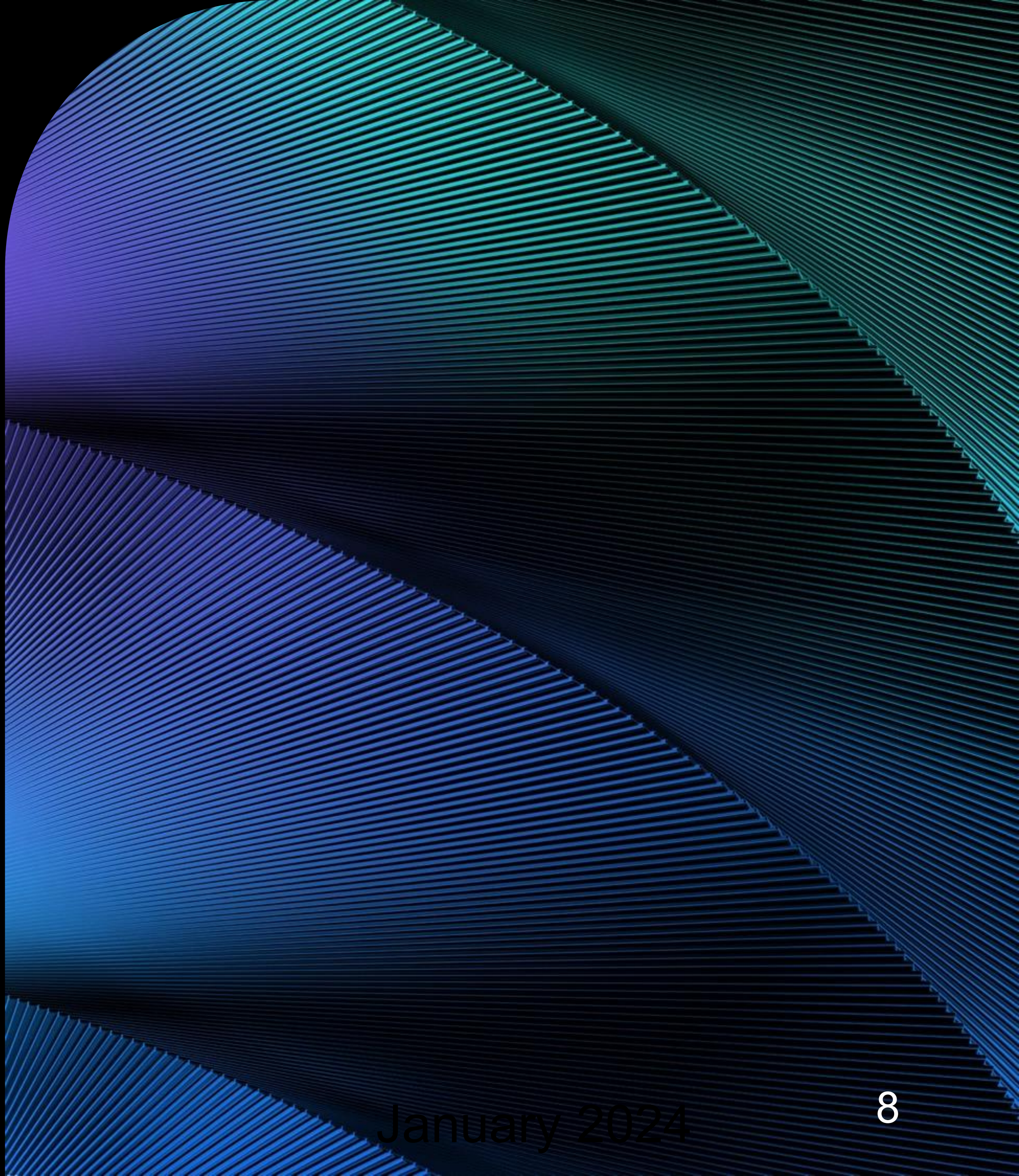
What are some of the challenges?

- Existing approaches to “qualification” of software components (e.g. Part 8-12) were for historical use cases
- When a component is identified at a particular level in an architectural design
  - Identify an existing component that addresses its needs (e.g. its safety requirements) **or**
  - Do further design on this component
- Any existing component to be used has to be shown to be “suitable” i.e. can it fulfil
  - The allocated safety requirements **with**
  - Their assigned ASIL value **and**
  - Architectural properties such as freedom from interference
- Existing components can include one reused from a previous project, or a so-called “safety element out of context”, or even an off-the-shelf component that may not have a safety pedigree
  - Desire to use complex pre-existing software (e.g. open-source software including but not limited to Linux)

What else is happening?

- Related standards e.g. ISO 21448 (SOTIF), ISO/SAE 21434 (cybersecurity)
  - How do we manage dependencies, synergies and even conflicts between the requirements of these standards?
- New documents supporting ISO 26262 e.g. use of complex pre-existing software (ISO/PAS 8926)
  - How do we integrate these into the next edition of ISO 26262?
- Standards emerging to support new disciplines e.g. safety of automated driving (ISO/TS 5083), safety of AI (ISO/PAS 8800)
  - Some of the wider spaces e.g. in AI are very fast moving and many standards being developed
  - How to keep these aligned with ISO 26262 etc.?

Conclusions and questions



Dr David Ward
MA PhD CEng CPhys MInstP MSAE
Global Head of Functional Safety

D +44 (0)24 7635 5430
E david.ward@horiba-mira.com

HORIBA MIRA Ltd.
Watling Street
Nuneaton
Warwickshire
CV10 0TU
United Kingdom

www.horiba-mira.com