

# Standards for road vehicle automation – are we nearly there yet?

**Dr David Ward**

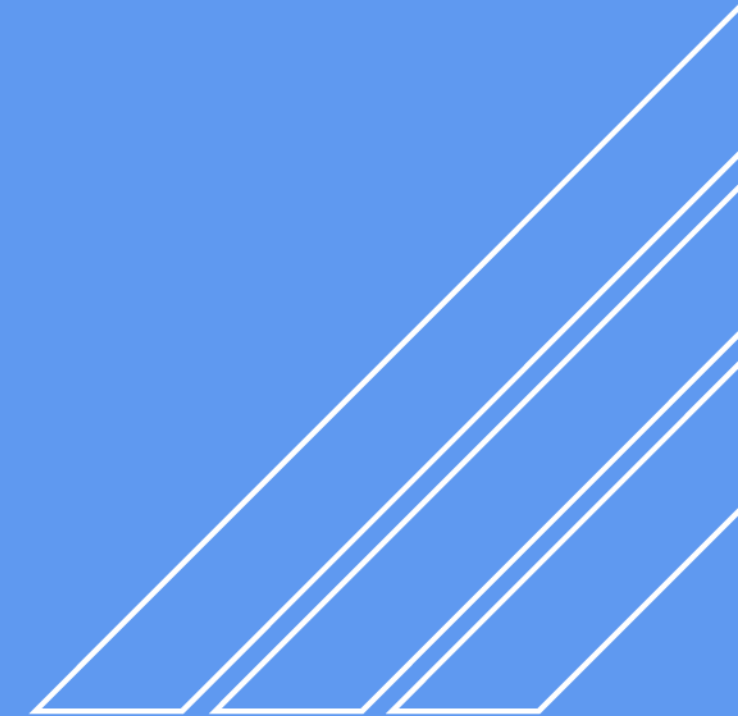
Senior Technical Manager – Functional Safety

May 2019

- 
- Background and context of automated driving features in road vehicles
  - Functional safety, SOTIF and the wider system safety context
  - Why do we have standards?
  - Current status of standardization
  - What do we perceive the gaps (opportunities) are?
  - Conclusions and future outlook

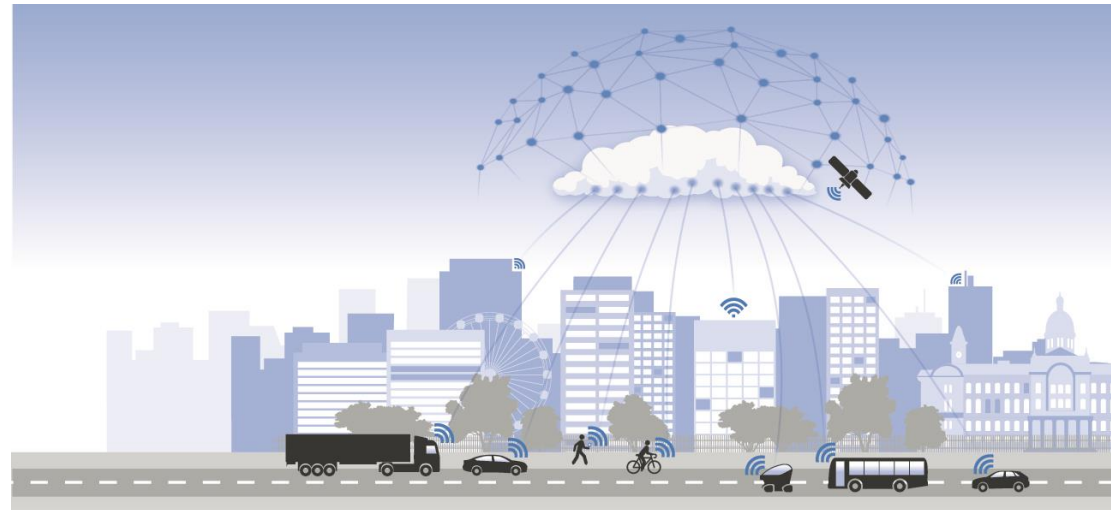


# Background and context of automated driving features in road vehicles

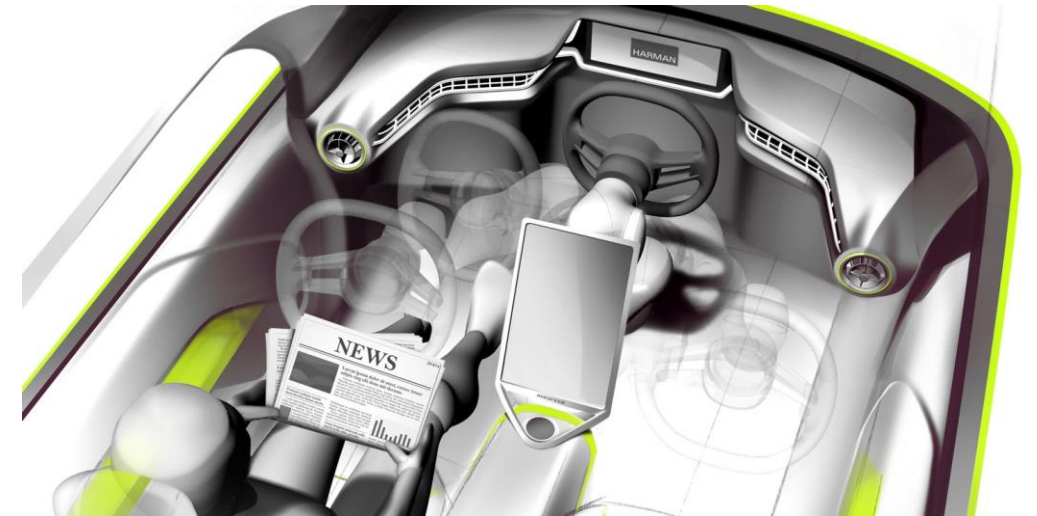


# Automotive “megatrends”

## ■ Connected



## ■ Automated



## ■ Electrified

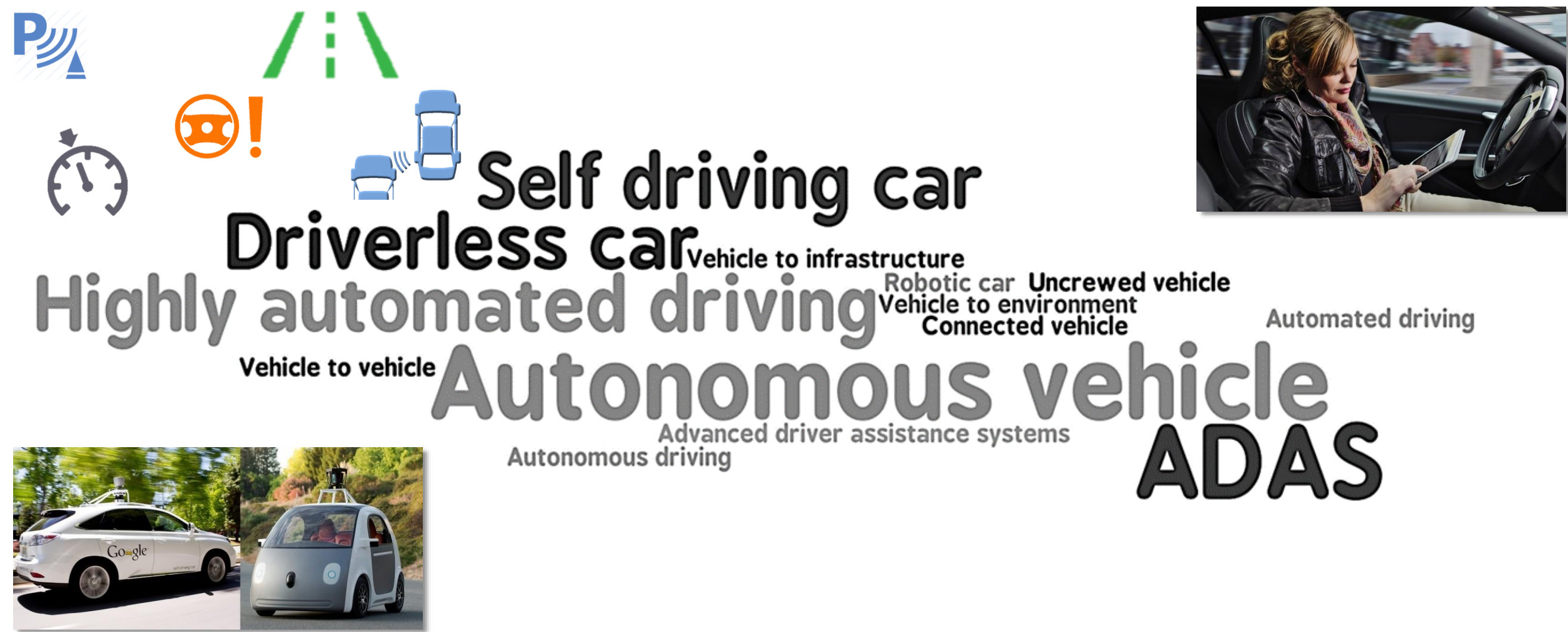


## ■ Shared





# So what exactly does “automation” mean?






















# Examples of automated features / vehicles



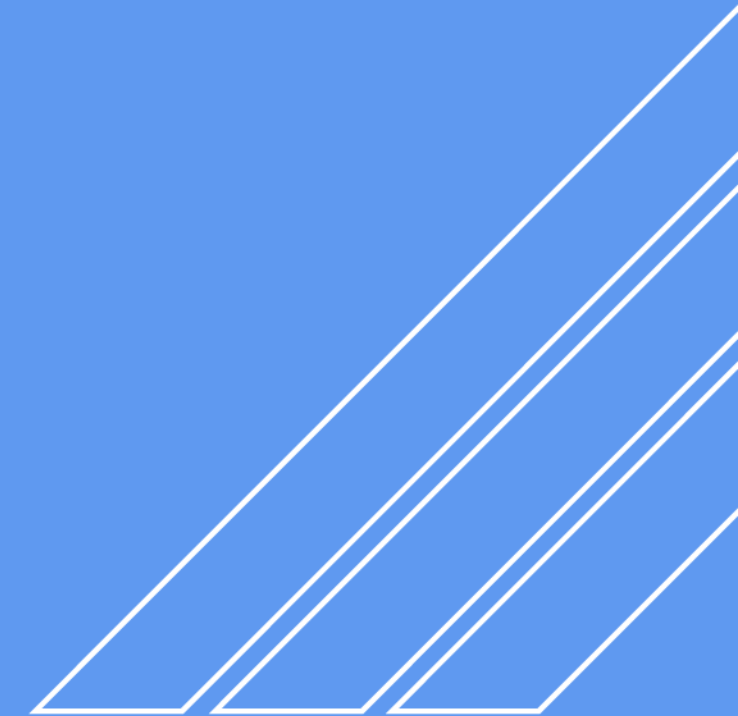


# Vehicle automation

Source: SAE J3016 (modified)

		Steering and acceleration/ deceleration	Monitoring of driving environment	Fallback when automation fails	Automated system is in control	
Assisted driving	0 NO AUTOMATION				N/A	Examples: LDW, FCW
	1 DRIVER ASSISTANCE				SOME DRIVING MODES	Examples: LKA, ACC
	2 PARTIAL AUTOMATION				SOME DRIVING MODES	Example: TJA
Delegated driving	3 CONDITIONAL AUTOMATION				SOME DRIVING MODES	Example: Highway “pilot”
	4 HIGH AUTOMATION				SOME DRIVING MODES	Examples: AVP, ride share
	5 FULL AUTOMATION					Example: “Google car”

# Functional safety, SOTIF and the wider system safety context





# Scope of product safety vs. functional safety and security

ISO/SAE 21434  
(in preparation)

Cybersecurity

Functional  
safety

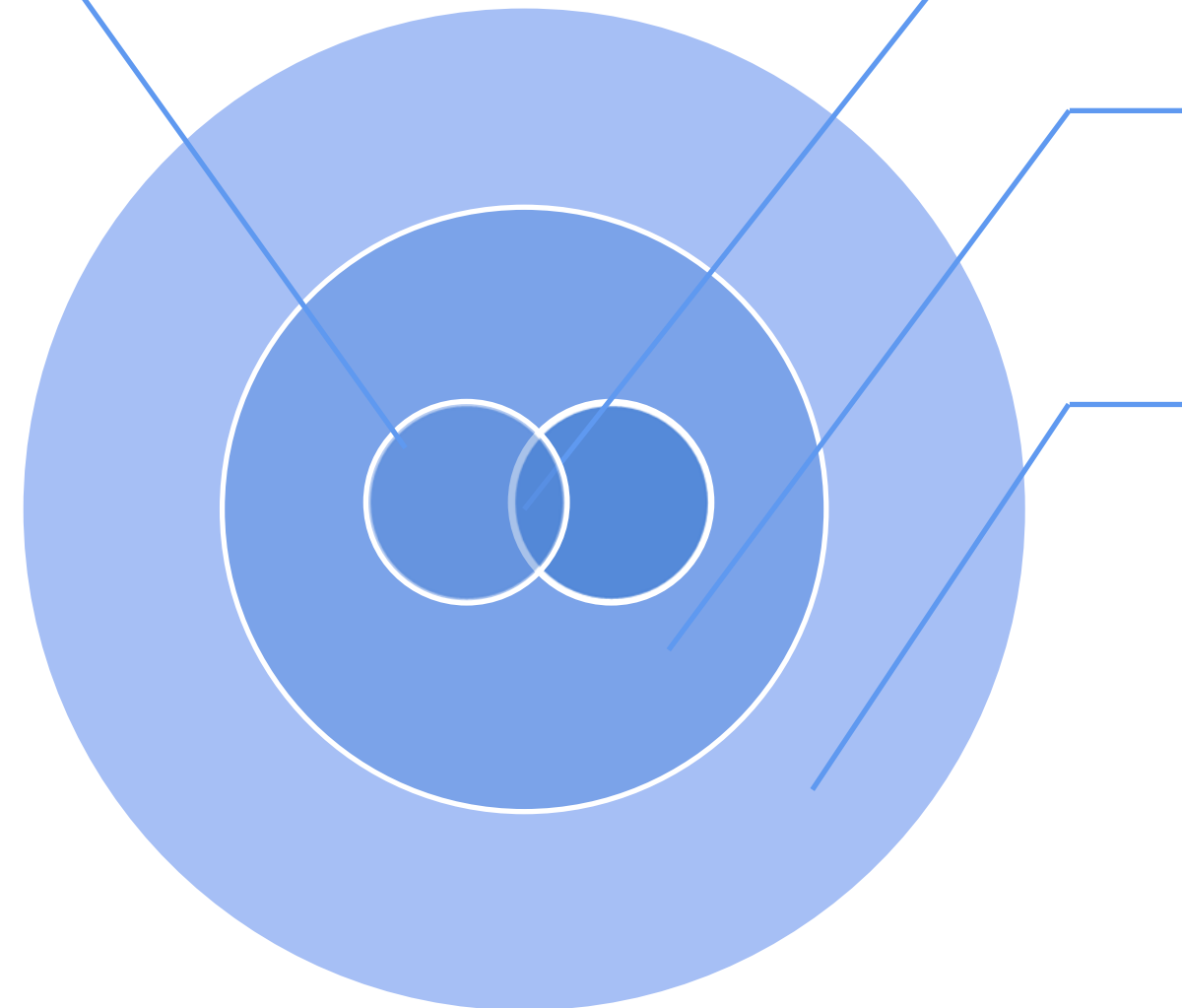
ISO 26262

System  
safety

e.g. SOTIF  
(ISO/PAS 21448)

Product  
safety

e.g. IATF, legislation  
(FMVSS, Type Approval)



# Achieving Vehicle Resilience

The scope of **FS**, **CS**, **SOTIF** (ISO/PAS 21448), and **INTEROPERABILITY**

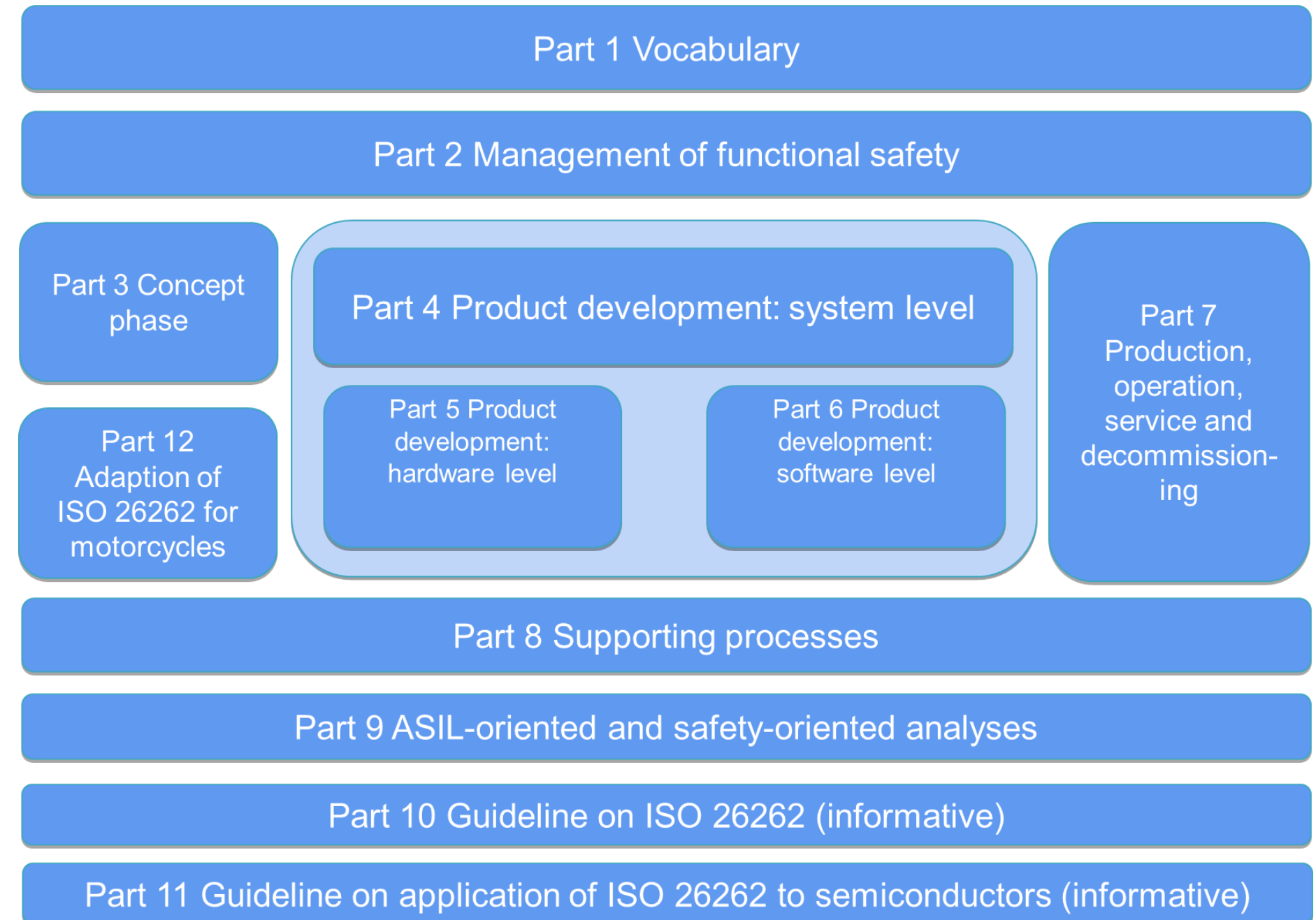


Source	Cause of hazardous event	Within scope of
E/E system factor	E/E system failures	ISO 26262
	Performance limitations, insufficient situational awareness with or without reasonably foreseeable misuse	SOTIF
	Reasonably foreseeable misuse, incorrect HMI (e.g. user confusion or overload)	SOTIF European statement of principles on HMI
	The system technology	Product-specific standards
	E/E system interference, e.g. connectivity issues	Interoperability engineering
External factor	Security violation	SAE J3061 or ISO/SAE CD 21434
	Impact from active infrastructure and/or vehicle to vehicle communication, external devices and cloud services	ISO 20077 ISO 26262
	Impact from car surroundings (other users, “passive” infrastructure, environment: weather, EMC...), e.g. EM susceptibility	SOTIF ISO 26262 Interoperability engineering



# Brief summary of ISO 26262

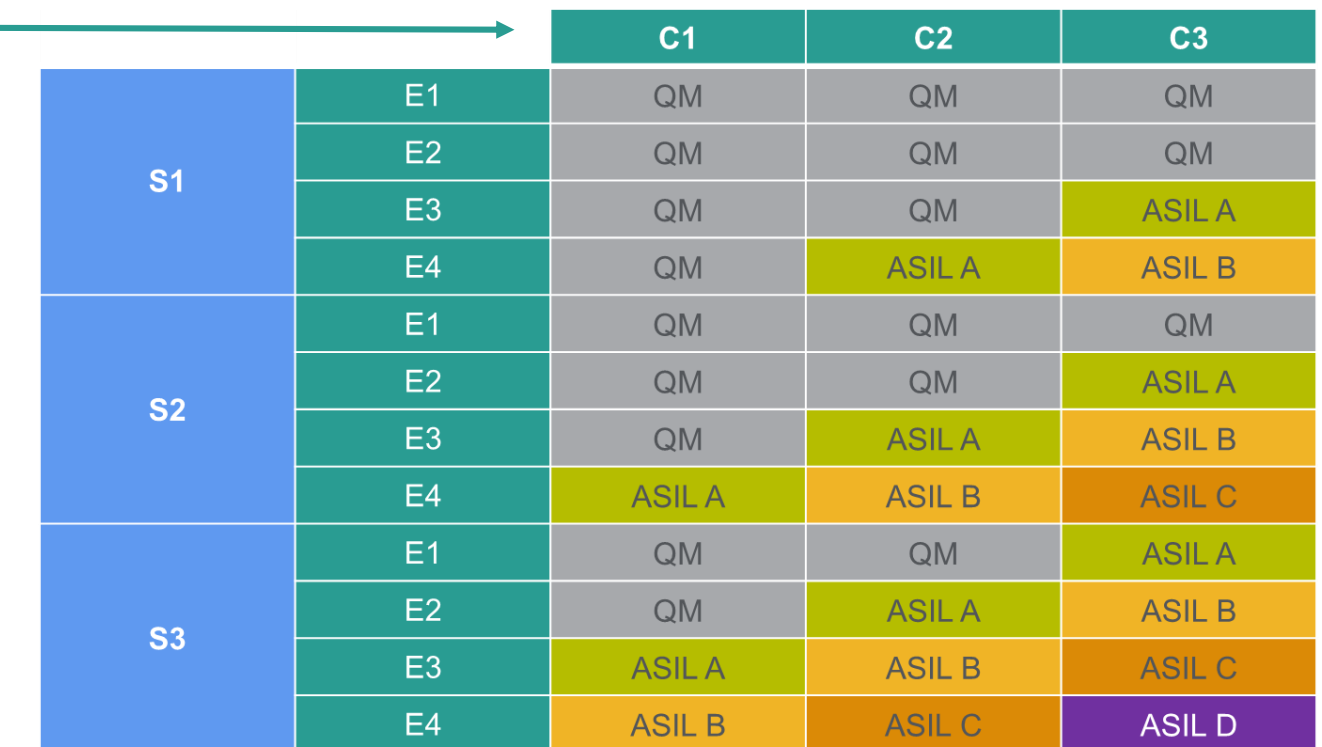
- First published in 2011, ISO 26262 is considered to represent the “state of the art” for development of vehicle electronic systems
- Derived from IEC 61508 but more of an interpretation than a direct sector-specific version



# Brief summary of ISO 26262

## Key assumptions in the standard

- Physical architectural view of vehicle electronics
  - Particularly reflected in the concept of the “item” (which is closely aligned to traditional supply chains and procurement practices)
- Driver assumed to be present and in final control, so “controllability” is frequently used to argue down risk
  - Systems that “just” give warnings for “comfort and convenience” purposes e.g. TPMS are generally not considered safety-relevant (despite legislation ...)
  - “Fail silent” as safe state
- Some driving situations are considered rare so “exposure” is frequently used to argue down risk



		C1	C2	C3
S1	E1	QM	QM	QM
	E2	QM	QM	QM
	E3	QM	QM	ASIL A
	E4	QM	ASIL A	ASIL B
S2	E1	QM	QM	QM
	E2	QM	QM	ASIL A
	E3	QM	ASIL A	ASIL B
	E4	ASIL A	ASIL B	ASIL C
S3	E1	QM	QM	ASIL A
	E2	QM	ASIL A	ASIL B
	E3	ASIL A	ASIL B	ASIL C
	E4	ASIL B	ASIL C	ASIL D



# What does ISO 26262 say about wider safety concerns?

- Scope of ISO 26262 is (deliberately) narrow compared to wider product safety
  - Definitions of **harm** and **hazard** are very specific
  - Scope statements exclude functional performance etc. and also exclude certain hazards
    - Electric shock, fire, smoke, heat, radiation, toxicity, flammability, reactivity, corrosion, release of energy (and similar)
    - Many of these are **specific hazards** or **particular hazards** associated with the technology
- Example: electric vehicle
  - Relevant product safety regulations include Reg 100 (electrical safety), Reg 94/95 (crash), ...

# Does that mean ISO 26262 ignores wider concerns – NO!

- Narrow scope of functional safety
  - But note introductory remark that “[ISO 26262] also provides a framework within which safety-related systems based on other technologies can be considered”
- Acknowledgement of common development procedures
  - Reference to safety being “intertwined” in introduction and explicit acknowledgment e.g. Part 6
- Addressing hazards out of scope
  - Part 3 Clause 6.4.2.4 requires these to be addressed through the relevant organizational procedures
- New requirement to “institute and maintain effective communication channels” with other disciplines – cybersecurity given as a specific example
  - Notable that this is part of requirements for a safety culture in Part 2



# Why do we have standards?



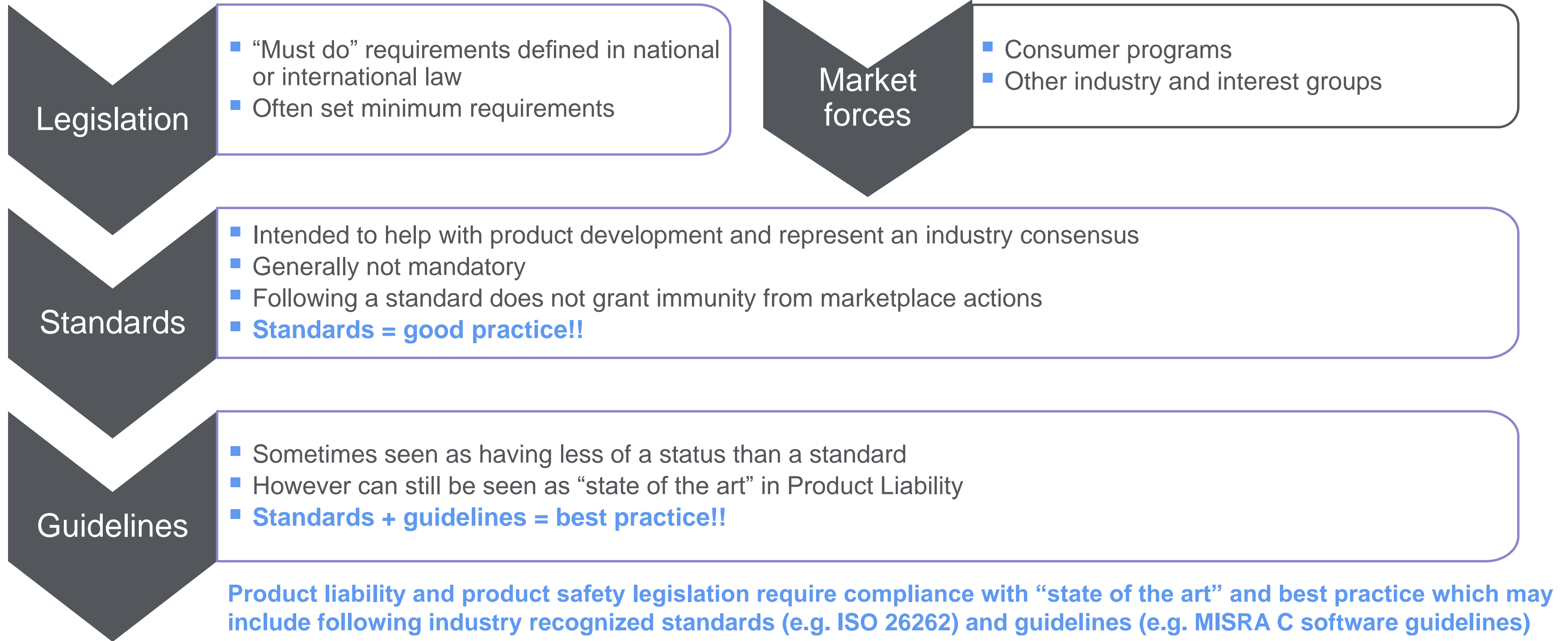
# Why do we have standards?

- Standards allow a community of users to specify a baseline or state-of-the-art and facilitate cooperation within the industry and with other stakeholders (e.g. regulators)
  - Frequently want to have a “common language” in the supply chain
    - ASIL in functional safety is a good example of this (even if it has become hackneyed)
  - Product manufacturers and suppliers are able to provide evidence that they have done their duty and followed recognized best practice and “state of the art”
  - Can provide the basis for independent assessment and similar activities (generally “internally” in automotive at present; to be continued ...)
- However standards alone do not result in a “safe product”
  - We have seen all too often a “checkbox” mentality to meeting the requirements of ISO 26262



# Legislation, standards and guidelines

How do they relate to each other?



- UNECE World Forum for Vehicle Regulations has developed recommendations for new regulations for cybersecurity and for software updates
  - Earliest date for legislative implementation November 2019 but late 2020 more likely
  - Both draft regulations will require an “approval authority” or “technical service” to carry out a “preliminary assessment” [i.e. an audit] of the management system (CSMS or SUMS) and issue a Certificate of Compliance
    - For cybersecurity, management system assumed to be audited against ISO/SAE 21434
    - For software updates, this was the motivation for proposing ISO 24089 as a new work item
  - “Test phase” currently planned to attempt trial applications of CSMS “assessment” using a draft of ISO/SAE 21434

# Legislation case study – cybersecurity

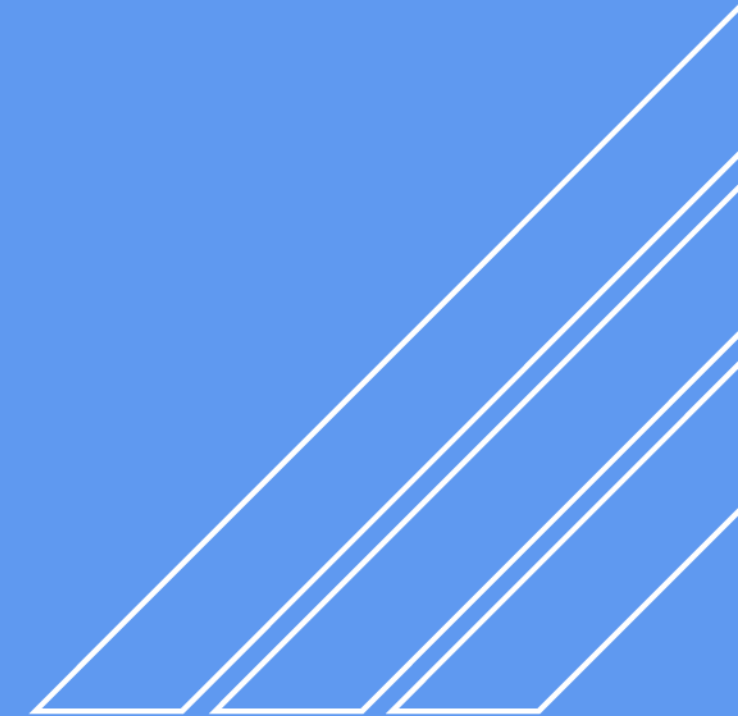
## European Cybersecurity Act

---

- Proposed European legislation
  - Gives a permanent mandate to ENISA (European Agency for Network and Information Security) to act as the EU's Cybersecurity Agency
  - Creates a framework for European Cybersecurity Certificates for products, processes and services
    - Although these will initially be voluntary, possible mandatory application in the future
    - Approaches will depend on defined assurance level (“basic”, “substantial” or “high”)



# Current status of standardization



# Some current international standardization activities

Working group	Subject and publications	Latest status
ISO WG8	Functional safety – ISO 26262	Edition 2 Dec 2018
ISO WG8	SOTIF – ISO 21448	PAS Jan 2019  Development of full standard now underway
SAE	Cybersecurity guidebook – J3061™	Published Jan 2016
ISO/SAE JWG11	Cybersecurity engineering – ISO/SAE 21434	CD with DIS due late 2019
ISO WG12	Software updates – ISO 24089	Work only just starting

# Updates to ISO 26262

## A frequently asked question ...

- ISO 26262 was officially published on 15 November 2011
- Almost immediately on 16 November 2011 ...



- 17 December 2018 ... Edition 2 finally published!



# Why update ISO 26262?

- Specific requirements to adapt ISO 26262 to
  - Extend scope to other types of vehicles (motorcycles, trucks, buses)
    - Motorcycles new Part 12 in Edition 2
  - Give additional guidance on semiconductor devices (new Part 11 in Edition 2)
  - Address ADAS-related hazards caused by “safety of the intended functionality” (SOTIF)
    - Currently developed as a separate PAS (ISO/PAS 21448) and future standard
- Other challenges include
  - Addressing highly distributed architectures
  - Moves towards highly automated vehicles
  - Cybersecurity

# Some key changes in ISO 26262 Edition 2

- Linkage with other disciplines e.g. cybersecurity, quality, mechanical engineering now acknowledged and explicit consideration required – significantly as part of requirements around a safety culture
- Confirmation reviews of key work products now have an “assessment” aspect, i.e. not just intended to be a “tick box” that the process of the standard was followed in developing them, but reviewing if they contribute to achieving functional safety
- Independent safety assessment can be based on a judgement of whether the objectives of the standard are met
- The safety case is now explicitly required to be based on an argument and some key technical activities are required to have an argument aspect to them (e.g. the technical safety concept)

# What are the gaps (opportunities!) in standardization?





# How is the industry approach to safety of electronic systems developing?

---

## ■ Past

- Driven by physical architecture, commodity-based approach
- Reflected in ISO 26262:2011

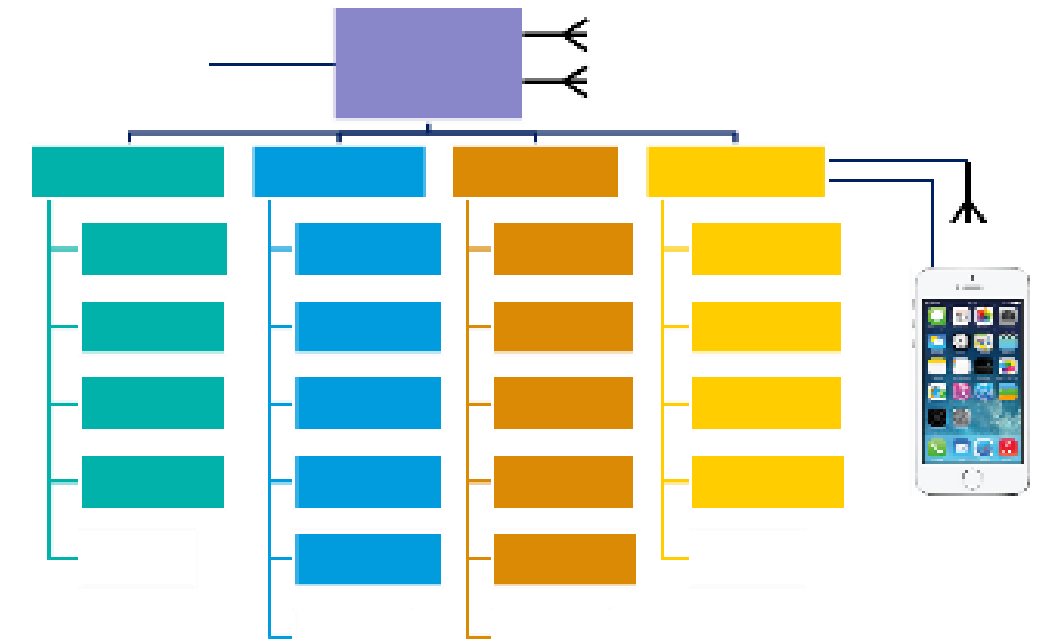
## ■ Examples

- “Powertrain control” is an “item” procured from supplier A
- “Brake control” is an “item” procured from supplier B
- Each contains a well-defined physical architecture (sensors, controller, actuators) and a well-defined set of functions
- Some (limited) interaction between them e.g. powertrain torque control during wheel-slip events

# How is the industry approach to safety of electronic systems developing?

## ■ Present

- Driven by logical architecture, feature-based approach
- Physical architecture is distributed
- ISO/PAS 21448:2019 (SOTIF PAS)
- ISO 26262 (“Edition 2”) retains physical architectural view although “objective-oriented” approach allows applicators (and assessors) flexibility



## ■ Examples

- “Items” include foundation brake control (ABS etc.), ACC, front AEB, rear AEB, brake hold
  - Each of these could cause the vehicle-level hazard “undemanded braking”
- Logical view during concept phase; translation to physical view during system design phase including collection, alignment and prioritization of safety requirements

# How is the industry approach to safety of electronic systems developing?

---

## ■ Future

- “Software defined car”??
  - Some manufacturers already proposing architectures with higher performance and flexible computing platforms overlaid on the base functions (such as powertrain control, braking which would retain traditional individual controllers, at least for now)
- ISO 26262 Edition 3? + SOTIF full standard + ???



# How do we treat machine learning / AI?

- Example: Ongoing SOTIF standard development considering this as a combination of ISO 26262 and SOTIF activities
  - ISO 26262 aspects:
    - Develop machine-learning software according to Part 6
    - Develop hosting hardware according to Part 5
    - Off-line training, application of “confidence in the use of software tools” (Part 8 Clause 11)
    - Training weights are considered “calibration data” (Part 6 Annex C)
    - Process FMEA on the off-line training process (e.g. avoid bias and limitation)
  - SOTIF aspects
    - Machine learning limitations (e.g. < 100% object recognition) through minimization of Areas 2 and 3

# Some topics (opportunities) to consider for the future

- A significant challenge is considering safety strategies and associated architectures for systems with availability requirements
  - Also how can we demonstrate “assurance” in these features and systems?
- Case study: SAE Level 3 Highway “pilot”
  - Permits “hands free” driving on highways / motorways but driver must take control when requested (e.g. when leaving the highway at an exit or in the case of failure)
  - Consider a system such as EPAS (electric power assisted steering)
  - In a conventional vehicle, if EPAS malfunctions then “fail silent” is considered the safe state as the driver “should” be able to maintain control through manual steering alone
  - In the context of a Level 3 feature EPAS is now an actuator and “fail silent” is not a suitable safe state ... at least not immediately

# Example safe state strategy for steering in Level 3 context

- ISO 26262 has (and has always had) the concept of a “warning and degradation strategy” which can cover multiple reactions including “safe” states and “emergency operation” **and significantly the transitions between them**
- Example strategy considering availability requirements of steering might include
  - Continued operation in presence of first fault without performance restriction – e.g. to at least complete current journey (may imply “fault tolerant” design of EPAS e.g. dual channel system)
  - Continued operation with degraded performance (e.g. speed limitation) and requirement for unscheduled maintenance
  - Continued operation with degraded performance and forced maintenance – e.g. to at least reach next junction or rest area then require breakdown assistance
  - “Stop as soon as safe” – move to shoulder (or as “final final” fall-back controlled stop in lane) using another system e.g. differential braking to control trajectory

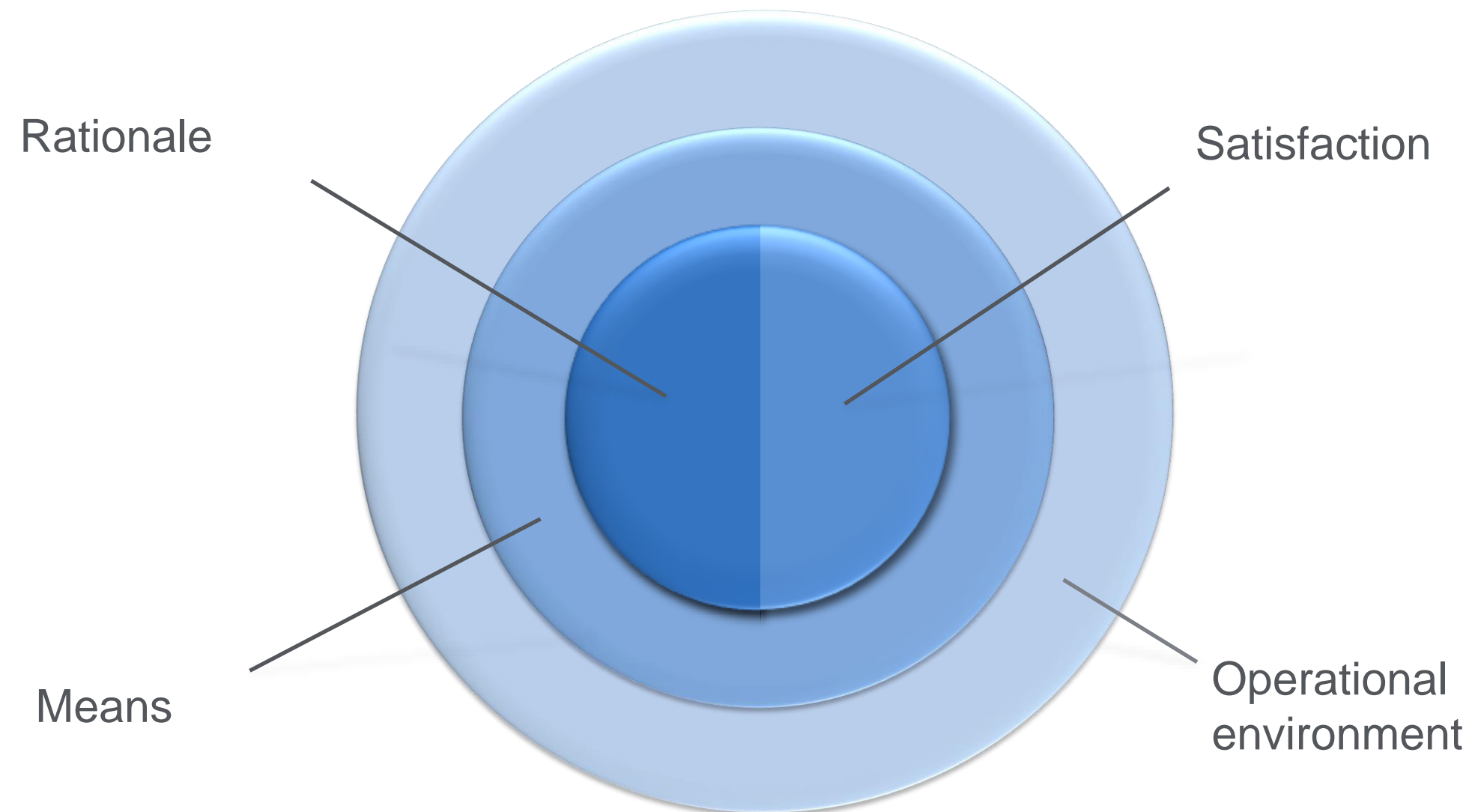
# Example architectural considerations

- ISO 26262 does not impose specific architectural solutions but instead provides tools and techniques to specify and evaluate required architectural properties
- Examples include
  - Independence – when architectural redundancy is required
  - Freedom from interference – typically when safety-related and non-safety-related functionality have to co-exist in the same context
  - Hardware architectural metrics – robustness against random hardware faults
  - Dependent failure analysis – to support specification and achievement of independence and freedom from interference
- Some of these techniques may need adapting for availability requirements but unlikely we can specify a “one size fits all” or “designated” architectures



# MISRA safety argument framework

Argument model – only for functional safety?



# Conclusions and future outlook towards Level 3 and higher levels of automation



- “Are we nearly there yet” – no, neither in terms of delivery of features to market nor the standardization that permits agreed industry approaches and a “common language”
- Standards need an agreed industry approach and consensus which is not always easy to achieve
  - “We are all in this together” – consensus needed amongst industry and wider stakeholders e.g. infrastructure operators, regulators
- There is much valuable work to be done however around safety strategies, architectures, new technologies such as AI and assurance activities

# Contact details



## Dr David Ward

MA (Cantab), PhD, CEng, CPhys, MInstP, MIEEEE, MSAE

Senior Technical Manager – Functional Safety

HORIBA MIRA Ltd.

Watling Street,  
Nuneaton, Warwickshire,  
CV10 0TU, UK

Direct T: +44 24 7635 5430  
E: david.ward@horiba-mira.com

T: +44 24 7635 5000  
F: +44 24 7635 8000

[www.horiba-mira.com](http://www.horiba-mira.com)