Transmitted by the expert from ISO

Informal document **GRVA-02-32**
2nd GRVA, 28 January – 1 Februar 2019
Agenda item 5(a)

The Safety of the Intended Functionality

Report on ISO/TC22/SC32/WG8 activities

Geneva, 31/01/2019

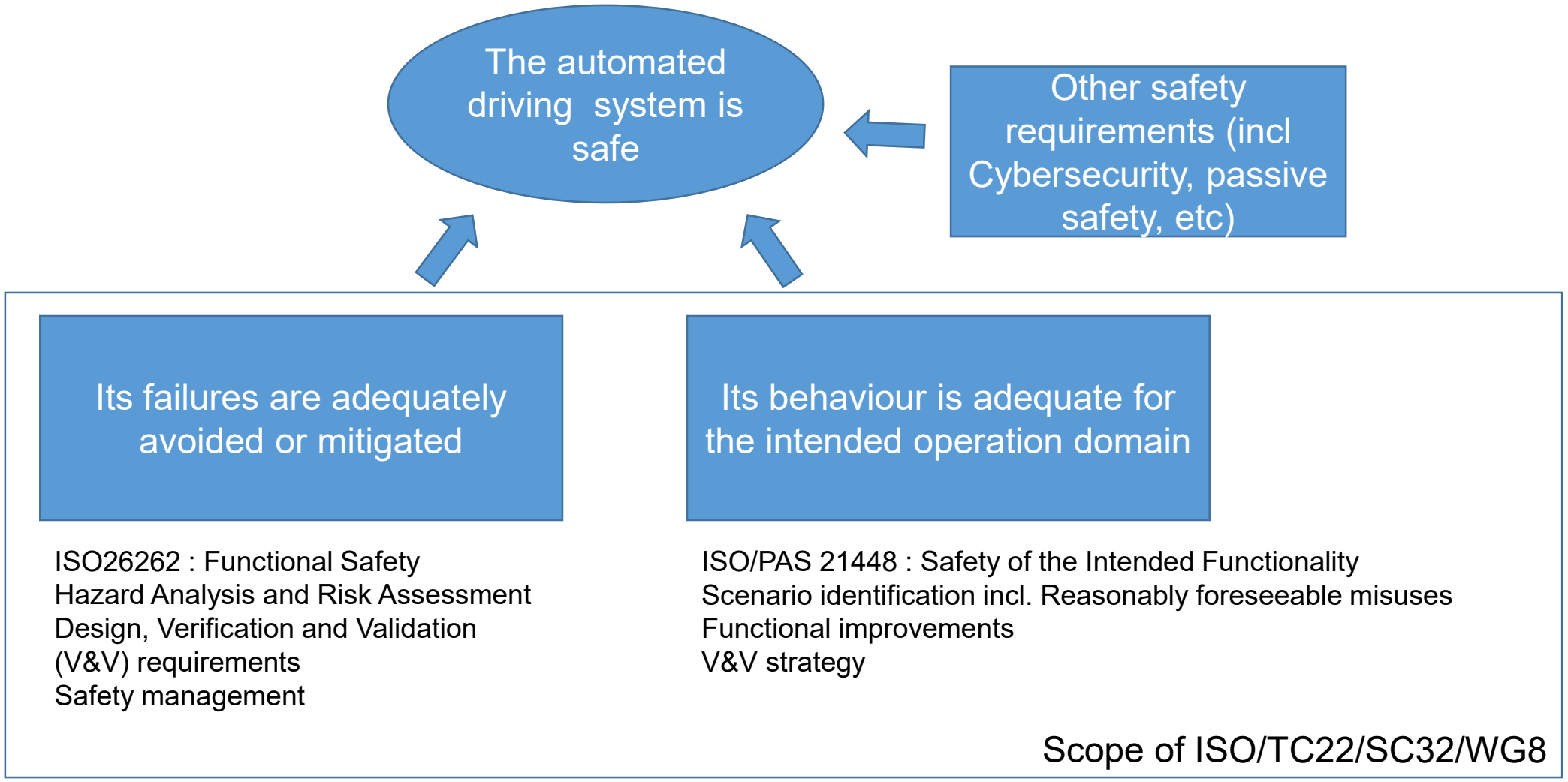
Nicolas Becker, ISO21448 project leader

Presented by
ISO/TC22/SC32/WG8

CONTENT

- Safety aspects of automated driving
- Motivation – What is the Safety of the Intended Functionality (SOTIF)?
- ISO/PAS 21448 status and activities
- Connection with Automated Driving (AD) regulatory activities
- Summary

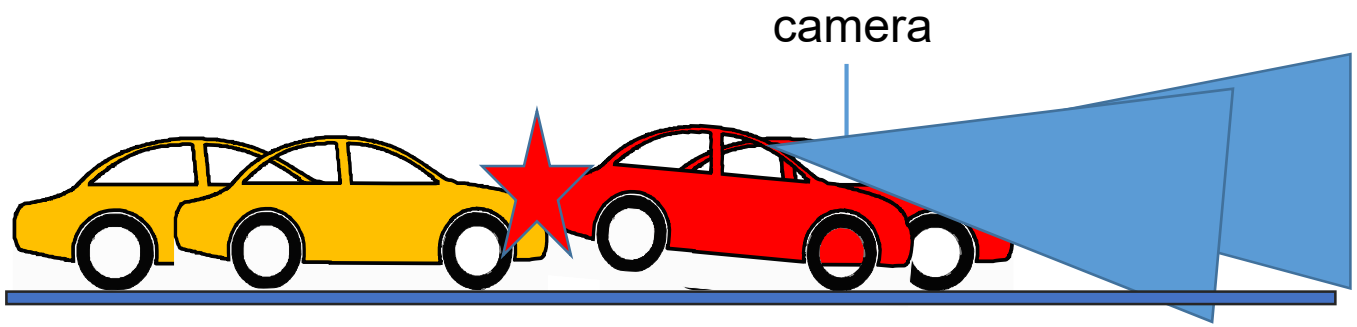
Safety aspects for an automated driving system



Presented by ISO/TC22/SC32/WG8

SOTIF EXAMPLE

Automatic emergency braking feature :



triggering events

unintended braking could be caused by limitations in perception system

- weather (rain/sun/fog)
- misinterpretation of image
- …

KEY ASPECTS OF 21448 - SOTIF

- ISO/PAS 21448 publication 01/2019
  - Focuses on driver assistance features with SAE automation levels 1 and 2
  - Covers potentially hazardous behavior under non-fault conditions
    - Caused by technological or system limitations
    - Includes evaluation of reasonably foreseeable misuse
  - Provides guidance for design, verification and validation measures
  - Issued as publicly available specification (PAS) (and not as an ISO standard) to enable fast publication
  - Includes high-level requirements on the objectives to achieve in the SOTIF analyses, and informative guidance on how to achieve them
- The work on ISO 21448 started in 11/2018
  - Extension to higher levels of automation (up to Level 5)
  - Significant interest in this work
    - 18 countries
    - 80 experts in Plenary featuring worldwide OEMs, Tier 1 and Tier 2 suppliers, and governmental institutes
  - Publication targeted for 2022

Presented by
ISO/TC22/SC32/WG8

CATEGORIZATION OF REAL-LIFE DRIVING SCENARIOS

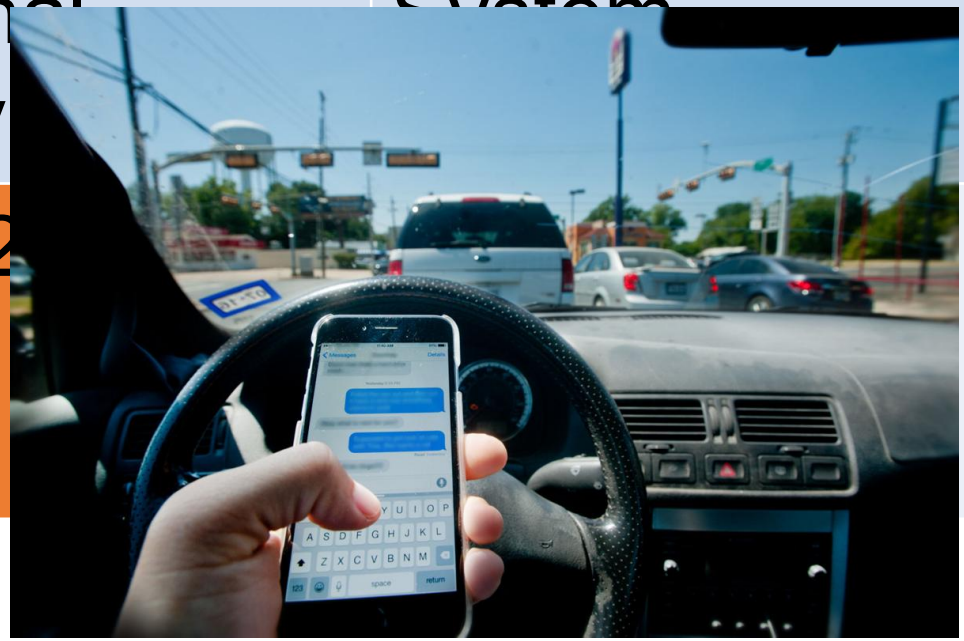
	Known	Unknown
Safe	Area 1 Nominal behavior	Area 4 System robustness
Potentially hazardous	Area 2 Identified system limitations	Area 3 “Black swans”

CATEGORIZATION OF REAL-LIFE DRIVING SCENARIOS

	Known	Unknown
Safe	Area 1 Nominal behavior	Area 4 System robustness
Potentially hazardous	Area 2 Identified system limitations	Area 3 “Black swans”

CATEGO S

	Nomin behav	
Potentially hazardous	Area 2	



CATEGORIZATION OF REAL-LIFE DRIVING SCENARIOS

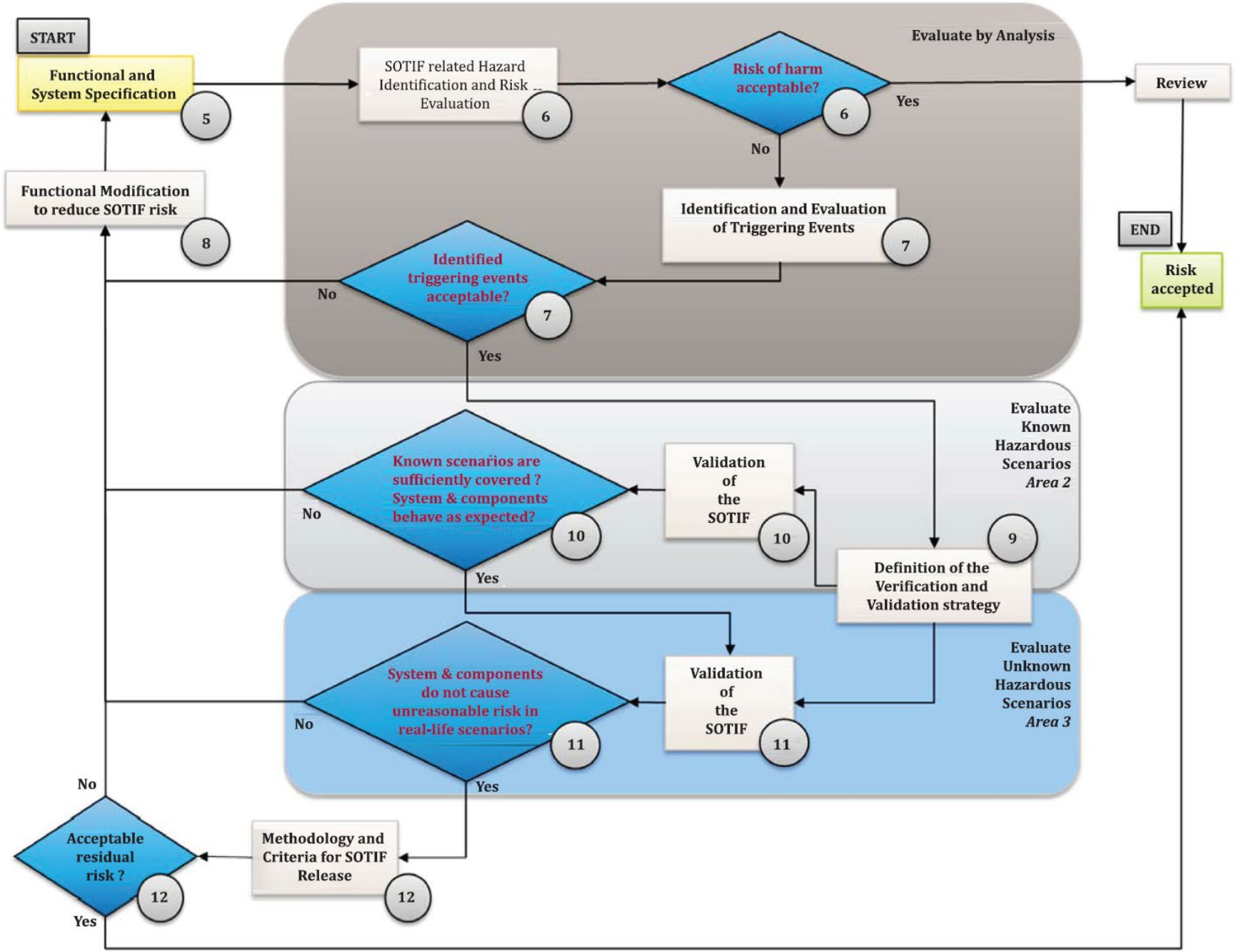
	Known	Unknown
Safe	Area 1 Nominal behavior	Area 4 System robustness
Potentially hazardous	Area 2 Identified system limitations	Area 3 “Black swans”

CATEGORIZATION OF REAL-LIFE DRIVING SCENARIOS

		Unknown
Safe		Area 4 System robustness
Potentia hazardo		Area 3

Presented by
ISO/TC22/SC32/WG8

Flowchart of SOTIF Activities (ISO/PAS 21448, Fig. 9)



Presented by
ISO/TC22/SC32/WG8

VERIFICATION AND VALIDATION ACTIVITIES

	Known	Unknown
Safe	Area 1 Normal validation	Area 4 Not applicable
Potentially hazardous	Area 2 V&V of the adequate behaviour of the system, incl. of the functional improvements	Area 3 Qualitative and Quantitative evaluation of the residual scenarios

RESIDUAL SCENARIOS EVALUATION – QUANTITATIVE APPROACH FOR AREA 3

- The ISO/PAS 21448 indicates that :
  - A quantitative target is defined for the demonstration that the unknown/unsafe scenarios are sufficiently implausible, e.g. a maximum probability of incorrect behavior per hour.
    - The PAS however does not specify normative quantitative target values
  - This quantitative target considers applicable regulations, standards and relevant traffic statistics.
  - The validation strategy shall provide demonstration that this target is met
- This quantitative approach is NOT a criteria that would allow to ignore a plausible potentially hazardous scenario : those must be addressed anyhow
- It is ONLY a criteria to claim sufficient validation coverage at the time of the beginning of customer activation of the functionality
- For a SAE level 1 or 2 functionality in the scope of the PAS, this leads to a validation strategy that is in the order of what a captured fleet can achieve
- For a SAE level 3+ functionality in the scope of the future ISO21448, the target derived through this approach are much more stringent., The validation will therefore require techniques in addition to the road tests, for instance a higher contribution of simulations. This is a primary topic for the future ISO21448.
- The procedure for the demonstration on how these targets are met is still a topic of discussion.

HOW CAN ISO21448 SUPPORT AV REGULATION?

- ISO 21448 will provide a consensus from the ISO experts on the framework to design and demonstrate the Safety of the Intended Functionality
- A first draft will be available for voting and commenting in 2020
- It will describe an integrated, scenario-based approach, for the demonstration of the safety of the intended functionality, contributing to the safety evaluation of automated driving systems
- The approach to ensure the safety of the intended functionality combines several activities :
  - Design–level analyses of the system, its performances and its operating environment
  - Qualitative and quantitative evaluations
  - V&V techniques based on **simulation**, **tests in specified scenarios**, and **captured fleet in real driving** to maximize coverage
  - Quantitative justification of sufficient validation, derived from comparable human-driven behaviour
  - It augments the ISO26262 guidance with non-fault conditions considerations.

OPEN DISCUSSION POINTS

- Requirements that should be confirmed in an AD regulation
  - Overall framework for SOTIF demonstration
  - Acceptance condition for the identified residual risks :Under which conditions of implausibility is a potentially potentially hazardous behavior acceptable? => Societal issue
  - Acceptance condition for the end-of-validation milestone : is the proposed argument for sufficient validation acceptable?

- Demonstration of compliance to future AD regulation
  - The intention of 21448 is to provide a demonstration framework to support the safety evaluation of an automated driving functionality

- What future connections between ISO and UN/ECE on the SOTIF?
  - How to ensure a continued exchange of knowledge and information between the GRVA and the ISO committee?