Submitted by the expert from ISO

Informal document **GRVA-11-36**
11th GRVA, 27 Sept.-1 Oct. 2021
Agenda item 4(e)

The Safety of the Intended Functionality

Report on ISO/TC22/SC32/WG8 activities

GRVA, Sept. 2021

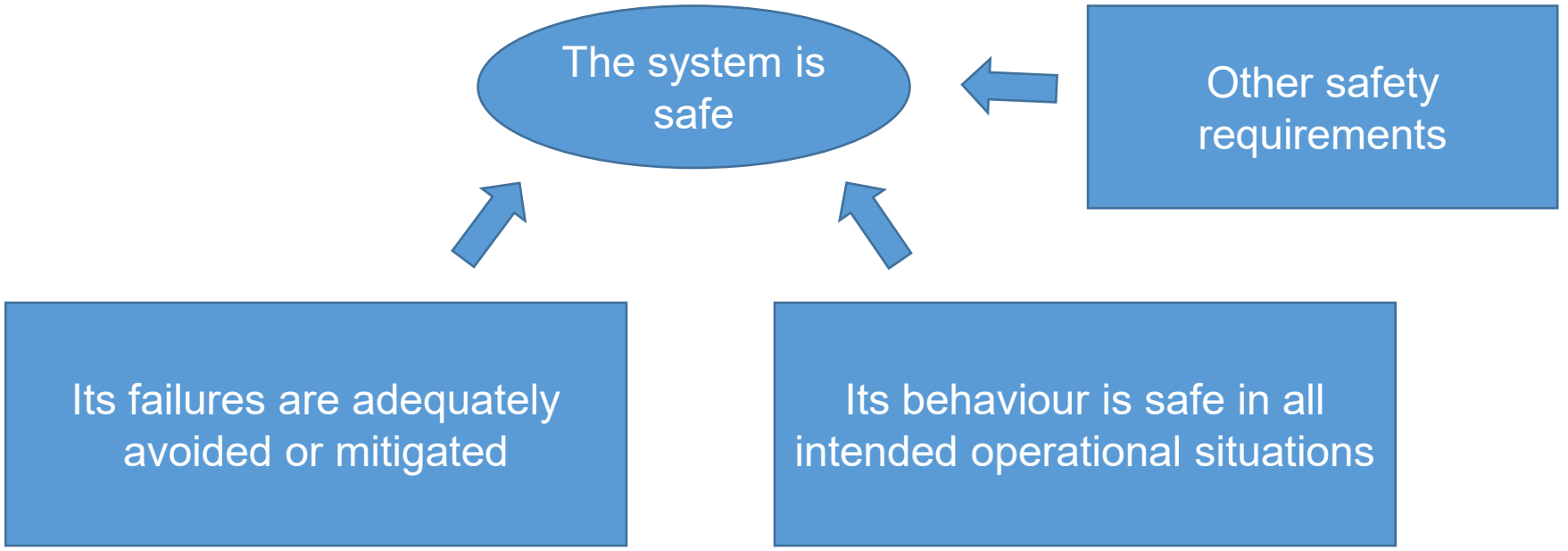
Nicolas Becker, ISO21448 project leader

Presented by
ISO/TC22/SC32/WG8

CONTENT

- Safety aspects of automated driving
- Motivation – What is the Safety of the Intended Functionality (SOTIF)?
- ISO/DIS 21448 status and activities
- Summary

Possible structure of the safety argument



ISO26262 : Functional Safety
Hazard Analysis and Risk Assessment
Identification of Faults and Failures
Design and V&V requirements
Safety management

ISO 21448 : Safety of the Intended Functionality
Scenario identification incl. Misuses
Identification of Functional Insufficiencies
Functional improvements
V&V strategy

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”

Presented by
ISO/TC22/SC32/WG8

TARGET OF THE ISO 21448 « SOTIF » STANDARD

- Provide a demonstration framework for the Safety of the Intended Functionality
- Same abstraction level as ISO 26262 (Method document, not solution oriented)
  - Other standardization intiatives are application-orientated, e.g. ISO TR 5083
- Consistent concepts and definitions with ISO 26262
- Avoidance of redundancies with ISO 26262
- Objective oriented : Compliance with the objectives is required, the methods to achieve them are informative
- Covering the whole vehicle lifecycle including the specification, design, verification, validation and operation phases

ISO-DIS 21448 STANDARDIZATION PROCESS AND STATUS

ISO/PAS 21448 published in 01/2019

- Scope limited to automation levels 0-2
- Extension of the scope for the future ISO 21448 standard to all automation levels
- Additional contents and methods are necessary

2021 status :

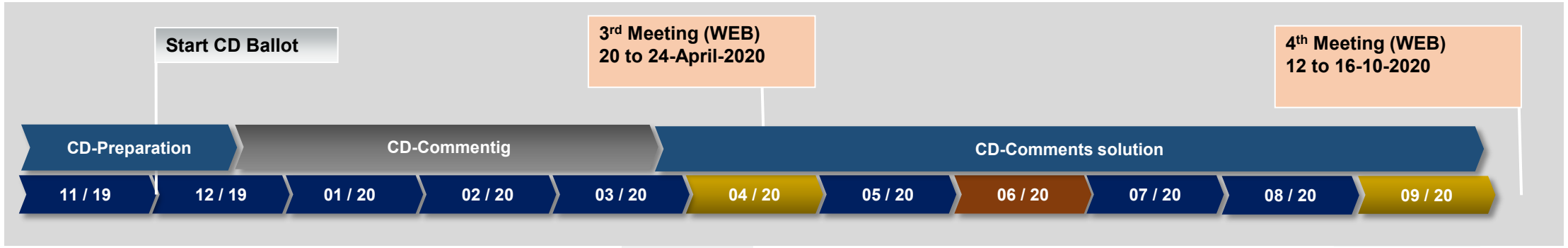
- The Committee Draft was published in December 2019, and commented through 2020
- The Draft of International Standard has been published end 2020, Commenting until Apr. 2021

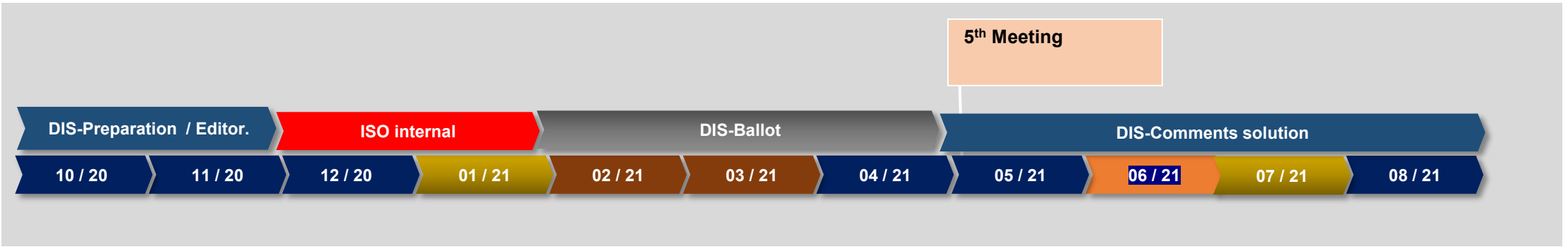
The DIS has been unanimously approved by the voting P-members

  - 21 Positive, Zero Negative votes
  - 1859 comments were received on the DIS (2626 received on CD)
  - Comments resolution will result in the FDIS, which should be delivered before the end 2021
- From this point, the DIS is public and may be used as a reference for implementation
- Publication still targeted in March 2022

Presented by
ISO/TC22/SC32/WG8

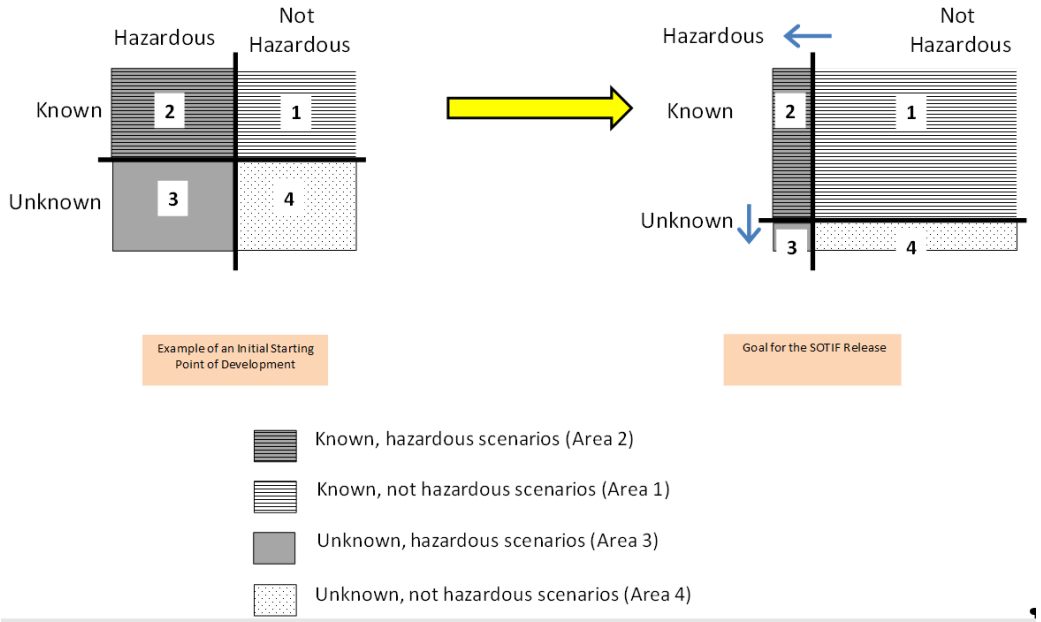
UPDATED TIMELINE

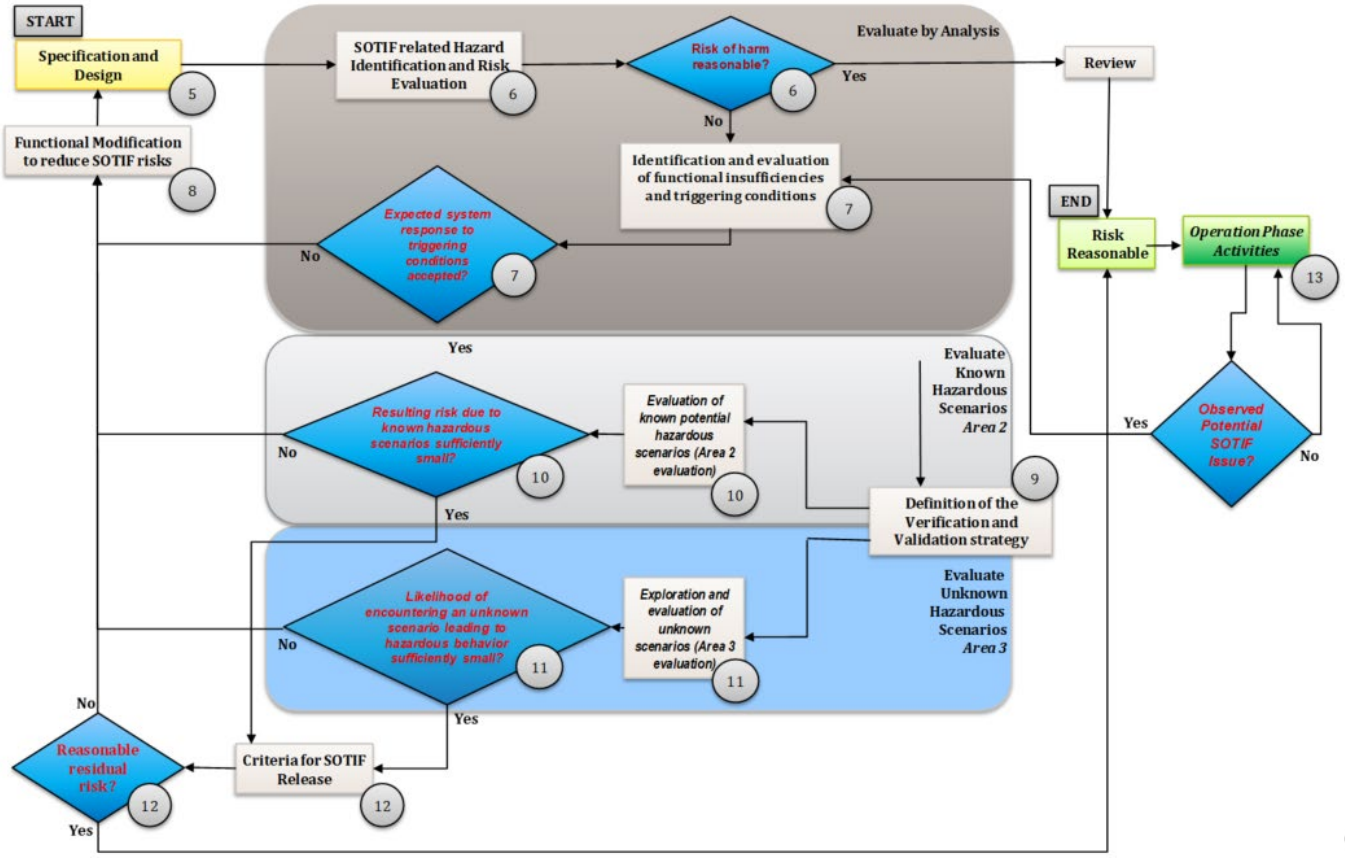




DIS 21448 – CURRENT STATUS

- Unchanged since the ISO PAS 21448 :
  - Scenario classification known/unknown, safe/hazardous, areas 1,2 and 3
  - Iterative concept of the development
  - Overall structure of the document

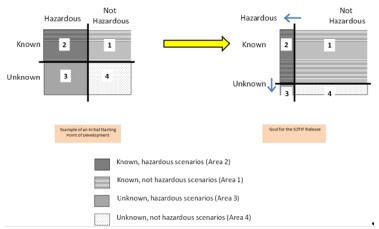


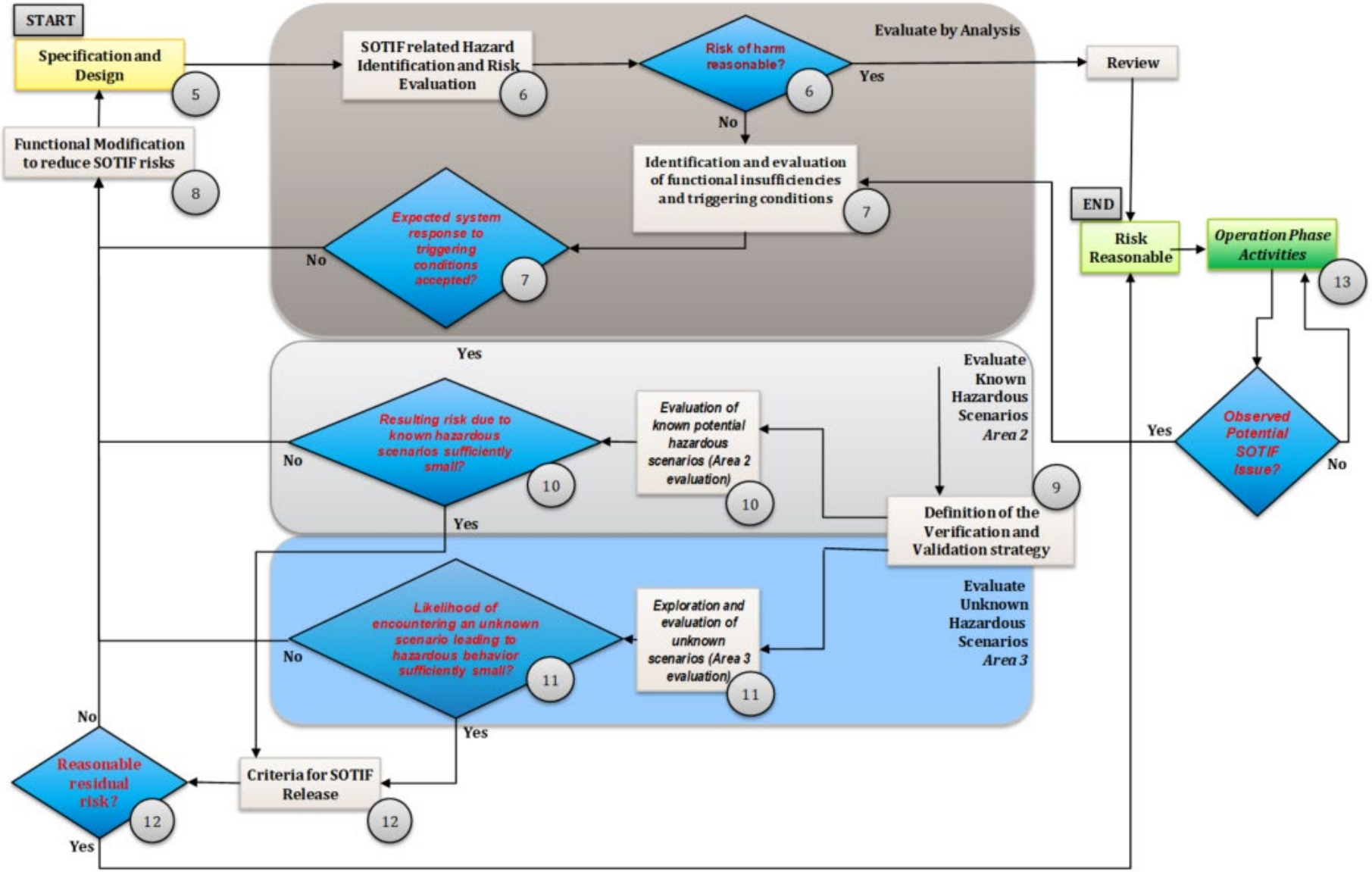


Presented by ISO/TC22/SC32/WG8

DIS 21448 – CURRENT STATUS

- Unchanged s
  - Scenario c
  - Iterative c
  - Overall str
    - Norma

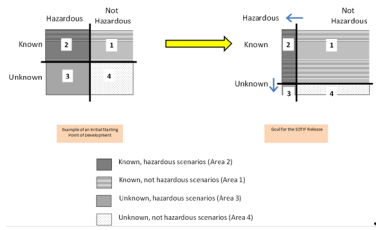


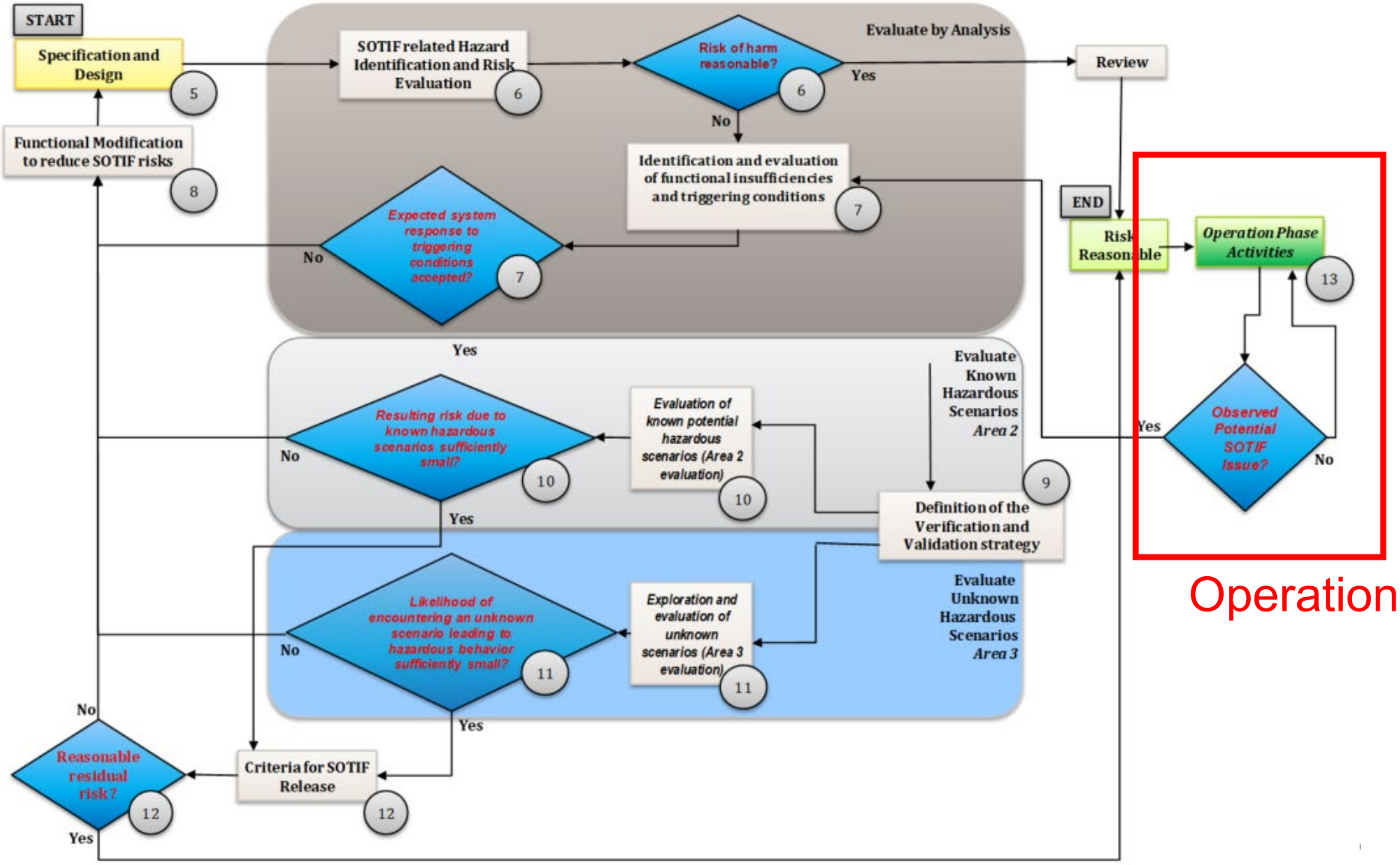


Presented by ISO/TC22/SC32/WG8

DIS 21448 – CURRENT STATUS

- Unchang
  - Scen
  - Iterat
  - Over
    - M





Operation

Presented by
ISO/TC22/SC32/WG8

HOW CAN ISO21448 SUPPORT AV REGULATION?

- It provides a consensus from the industry on the framework to design and demonstrate the Safety of the Intended Functionality
  - This includes the concepts for analyzing the scenarios, the triggering conditions and the functional insufficiencies of the system
- It supports a holistic, scenario-based approach, for safety demonstration
- It combines several arguments :
  - Design–level analyses of the system, its performances, its operating environment and its user interaction
  - Qualitative and quantitative evaluations of the system design
  - V&V techniques based on **simulation**, **tests in specified scenarios**, and **captured fleet in real driving** to maximize coverage
- It completes the ISO26262 guidance on functional safety

NEXT STEPS AND SUMMARY

- ISO 26262 and ISO 21448 address complementary aspects of system safety.

- The ISO/DIS 21448 is now the reference document. The PAS will be deprecated at IS publication.
- The DIS comments resolution is ongoing, the FDIS is expected for the end of this year.
- We are still on track for IS publication in March 2022, as per the initial schedule.

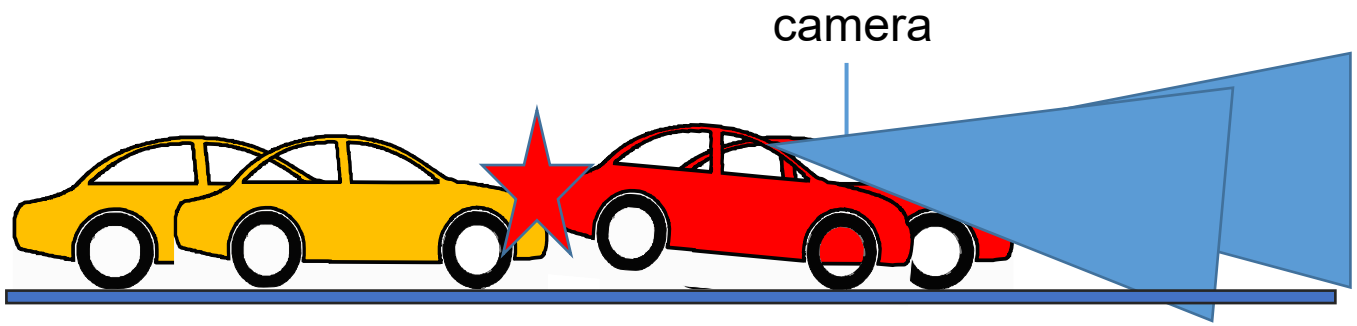
- Work to introduce some clarification regarding SOTIF in the edition 3 of ISO26262 will start end 2021.

- A number of additional initiatives in the field of AD safety have emerged (ISO TR 4804, ISO TS 5083, etc). Coordination is ongoing to keep these documents consistent, under the supervision of the ISO/TC22.

Backup

SOTIF EXAMPLE

Automatic emergency braking feature :



unintended braking could be caused by limitations in perception system

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

triggering events

DESIGN STAGE ACTIVITIES

- System definition
- Hazard analysis and acceptance criteria definition
- Analysis of the triggering conditions (incl. reasonably foreseeable misuse) and the functional insufficiencies of the system
- Definition of functional modifications to address those insufficiencies

VERIFICATION AND VALIDATION ACTIVITIES

- Definition of the V&V strategy
- For higher levels of automation, the acceptance criteria can be extremely high (human drivers are in the range of 10^{-7} severe accidents per hour)
  - A « brute force » demonstration by open road driving is unrealistic
- The SOTIF standards proposes several ways to show sufficient coverage for V&V:
  - Qualitative and quantitative justification of sufficient validation
    - Methods for defining an acceptance criteria and a validation target
    - Methods for defining and evaluating the verification and validation plan complying with that target, including :
      - ⇒ Analysis of the exposure to hazardous scenarios in case of misdetection
      - ⇒ Intensive simulations, e.g. Monte Carlo on sensitive parameters
      - ⇒ Staged tests
      - ⇒ Open road driving
      - ⇒ Taking benefit of the system architecture (e.g. sensors and algorithms redundancy)
- The quantitative evaluation is only a criteria to claim sufficient validation
- Any newly identified safety-related scenario must be analyzed and assessed