ktl Korea Testing Laboratory



International Standards Strategies for Securing Autonomous Driving Functions

Industrial Convergence Technology Center
Sungmin Kim

ISO 26262 2nd Edition Overview

Korea Testing Laboratory

ISO 26262 Standard Establishment Revision Activity

ISO 26262 1st Edtion

- ISO 26262 1st Ed Publication (2011.06)
  - Standardization on TC22 SC32 WG8

ISO 26262 2nd Edtion

- Drafting(2015.01) → CD Ballot(2016.02) → DIS Ballot(2016.12)
  → FIDS Ballot(2017.06) → IS (2018.01)
  - Revision work on TC22 SC32 WG8
- 2nd Ed Distribution(2018.12.24)

Ref.) CD(Committee Draft, DIS(Draft International Standard,
FDIS(Final Draft International Standard), IS(International Standard)

ISO 26262 2nd Edition Revision

Major Revisions

- Extend the range of road vehicles covered by the standard
  - (1st Ed) Safety-related systems that include one or more electrical and/or electronic (E/E) systems and that are installed in series production passenger cars with a maximum gross vehicle mass up to 3 500 kg
  - (2nd Ed) Safety-related systems that include one or more electrical and/or electronic (E/E) systems and that are installed in series production road vehicles, excluding mopeds
- Addition to ISO 26262 Application Guidelines for Semiconductor (Part 11)
- Increase in Multi-system based Items Related to Autonomous Driving
- Change of structure / Add / Complement / Integration of existing parts

ISO 26262 2nd Edition Revision

Major Revisions

- **Guidelines for applying ISO 26262-11 to semiconductors**

Agenda	Applicable systems
1) Base failure rate estimation - Permanent fault (IEC TR 62380, SN 29500, FIDES) - Transient fault - Component package failures 2) Dependent failure analysis 3) Fault injection	1) Digital components, memories 2) Analogue / Mixed signal components 3) Programmable logic device 4) Multi-core components 5) Sensors and transducers

SOTIF(Safety Of The Intended Functionality) Overview

ISO 21448 International Standard

ISO WD 21448 Road vehicles
- Safety of the Intended Functionality

ISO/TC 22 “Road vehicles”

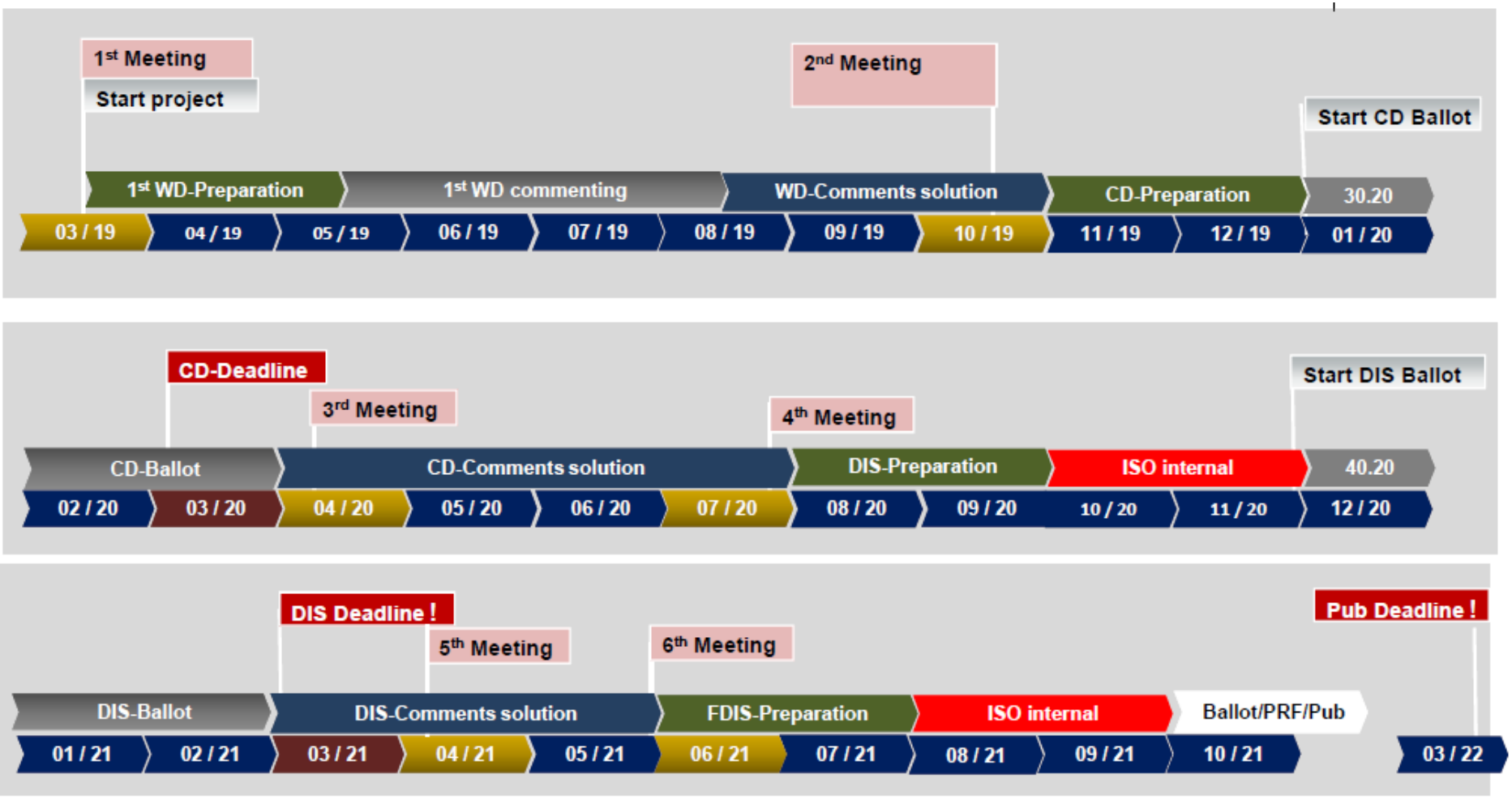
ISO/TC 22/SC 32 “Electrical and electronic components and general system aspects”

ISO/TC 22/SC 32/WG 8 “Functional Safety”

- TC (Technical Committee) / SC (Sub Committee) / WG (Working Group)
- KTL is a secretary of the Republic of Korea in ISO TC22/SC32/WG8 Functional Safety, responsible for providing guidance on verification, validation and design conformity required to achieve SOTIF.

ISO 21448 International Standard Pub Schedule

Project ISO 21448 Timeline



SOTIF Overview

SOTIF(Safety Of The Intended Functionality)

- SOTIF(Safety Of The Intended Functionality) : The Absence of unreasonable risk due to these potentially hazardous behaviours related to such limitations
- Functional safety : The absence of unreasonable risk due to hazards caused by malfunctioning behavior of E/E systems

To address the SOTIF, activities are implemented during the following 3 phases

1. Measures in the design phase

   Example : Requirement on sensor performance

2. Measures in the verification phase

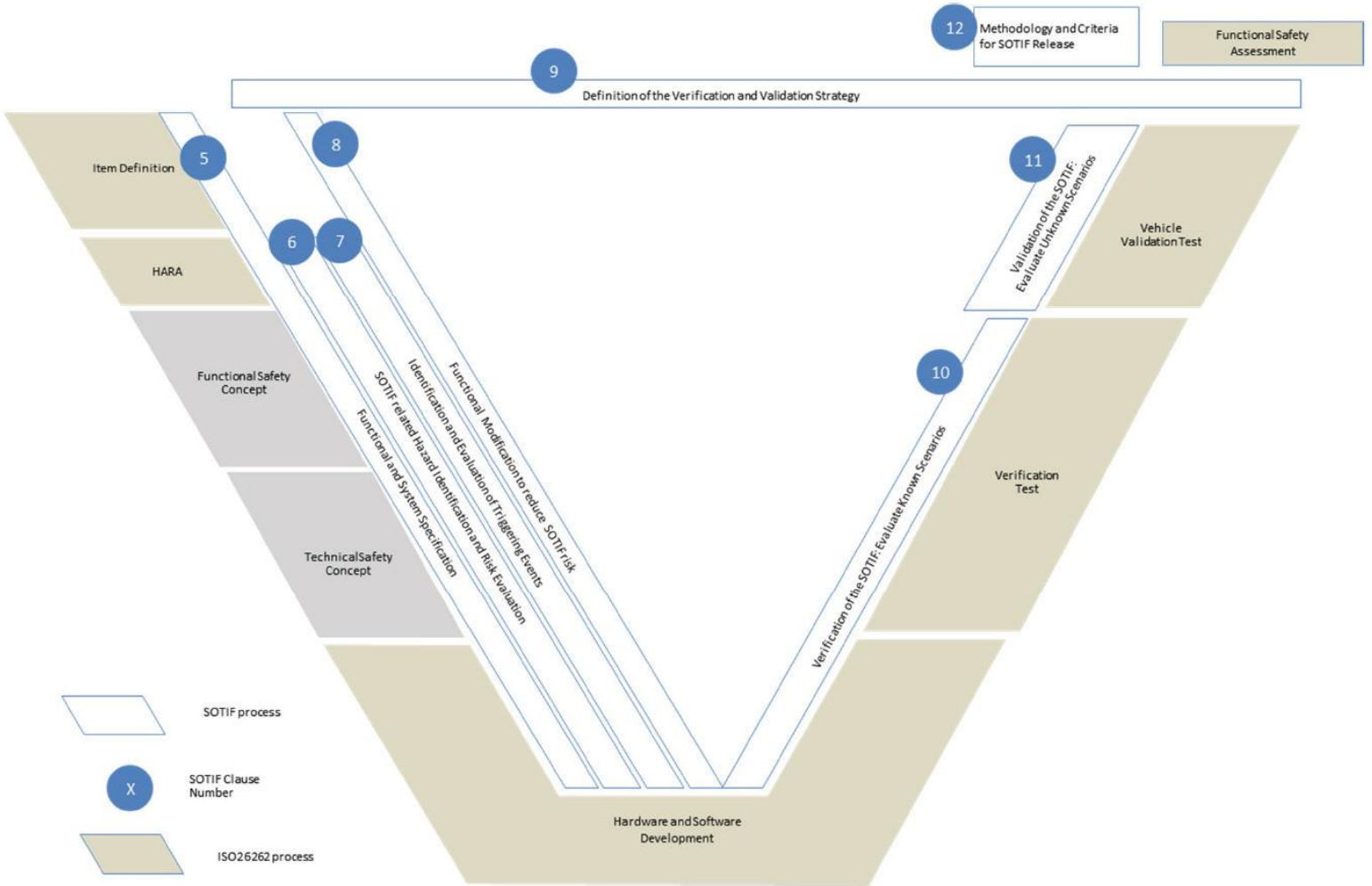
   Example : Technical Reviews, test cases with a high coverage of relevant scenarios, injection of potential triggering conditions, in the loop testing (e.g. SIL / HIL / MIL) of selected SOTIF are relevant use cases.

3. Measures in the Validation phase

   Example : Long term vehicle test, simulations

SOTIF Overview

Possible Interactions of Product Development activities between ISO 21448 and ISO 26262 processes



ktl Korea Testing Laboratory

SOTIF Standard Contents

◆ Overview of safety relevant topics addressed by different ISO standards

Source	Cause of hazardous event	Within scope of
System	E/E System failures	ISO 26262
	Performance limitations or insufficient situational awareness, with or without reasonably foreseeable misuse	ISO 21448
	Reasonably foreseeable misuse, incorrect HMI (e.g. user confusion, user overload)	ISO 21448 ISO 26262 European statement of principal on the design of human-achineinterface
	Hazards caused by the system technology	Specific standards
External factor	Successful attack exploiting vehicle security vulnerabilities	ISO 21434 SAE J3061
	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, environmental conditions: weather, Electro-Magnetic Interference…)	ISO 21448 ISO 26262

ktl Korea Testing Laboratory

Thank You