



2020 스마트시티 국가표준코디네이터

표준기반 R&D추진전략 성과보고회

자율주행차 안전/보안 표준 동향

백재원

(사)한국첨단자동차기술협회



목 차

- I. 자율주행차 안전/보안 관련 규제 및 표준
 1. 규제 및 표준의 목표
 2. 주요 표준화 기구
 3. UNECE WP.29
 4. ISO/TC 22/SC 32

- II. 자율주행차 안전/보안 관련 주요 표준
 1. Functional Safety & SOTIF
 2. Cybersecurity
 3. Software Update

- III. TC 22 신규 프로젝트
 1. TR 4804 소개
 2. TR 4804 구조
 3. Verification & Validation

자율주행차 안전/보안 관련 규제 및 표준

I-1 자율주행차 안전/보안 관련 규제 및 표준의 목표

"Safety & Cybersecurity" for Automated Driving



WP.29 GRVA
TFCS

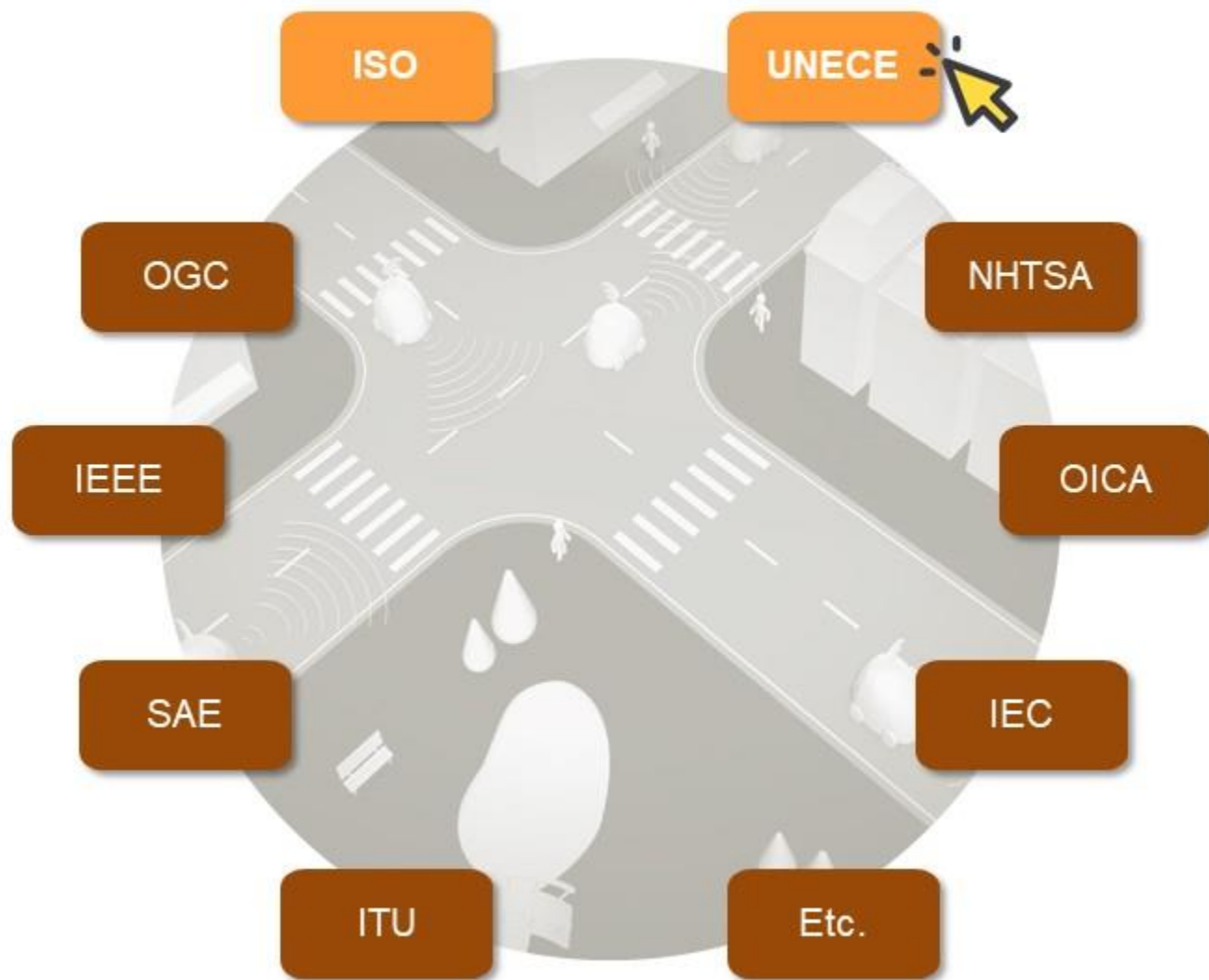


ISO/TC 22/SC 32
ISO 26262, ISO 21448,
ISO 21434, ISO 24089,
ISO 5112



ISO/TC 22
TR 4804

I-2 자율주행차 관련 주요 표준화 기구

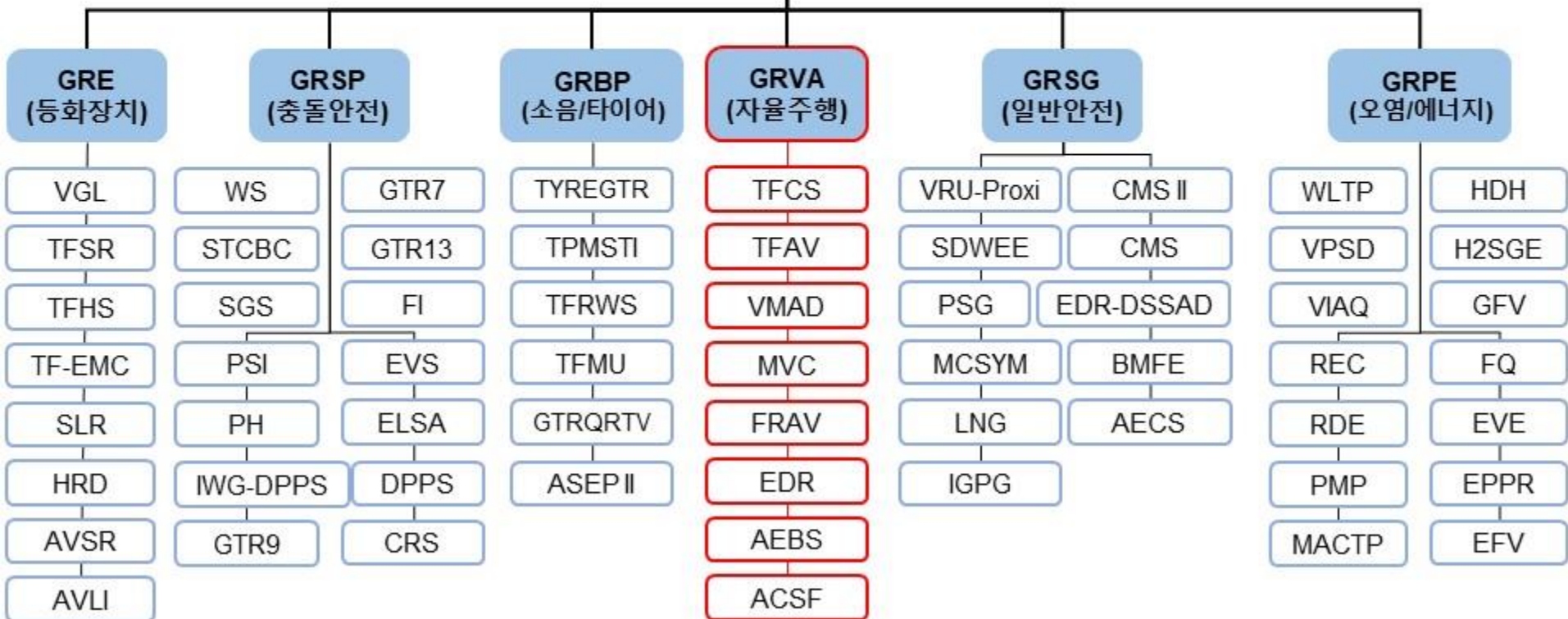


I-3 UNECE WP.29



WP.29

자동차 전문가 그룹



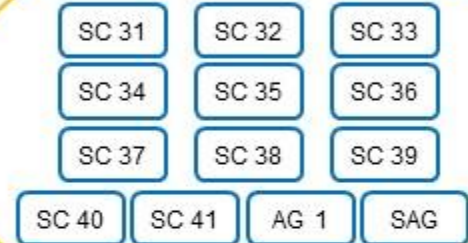
I-4 ISO/TC 22/SC 32

TC 22
Road vehicles



934개 표준 제정
(270개 표준 제정중)

SC 32 Electrical and electronic
components and general system aspects



총 74개의 WG이
운영되고 있음

REFERENCE	TITLE
WG 1	Ignition Equipment
WG 2	Environmental conditions
WG 3	Electromagnetic compatibility
WG 4	Automotive electrical cables
WG 5	Fuses and circuit breakers
WG 6	On-board electrical connections
WG 7	Functional characteristics of starting devices and electrical generators
WG 8	Functional safety
WG 9	Electrical connections between towing and towed vehicles
WG 10	Optical components - Test methods and requirements
WG 11	Cybersecurity
WG 12	Software update

2020.05 기준

I-3 UNECE – ISO mapping

UNECE



자율주행차 안전/보안 관련 주요 표준

II-1 Functional Safety & SOTIF (1/4)

ISO 26262 Functional Safety (2nd edition)

- **Functional Safety**
 - Absence of **unreasonable risk** due to **hazards** caused by **malfunctioning behaviour** of E/E systems
- **Unreasonable Risk**
 - risk judged to be unacceptable in a certain context according to valid societal moral concepts
- **Malfunctioning Behaviour**
 - failure or unintended behaviour of an item with respect to its design intent
- **E/E System**
 - System that consists of electrical and/or electronic elements, including programmable electronic elements



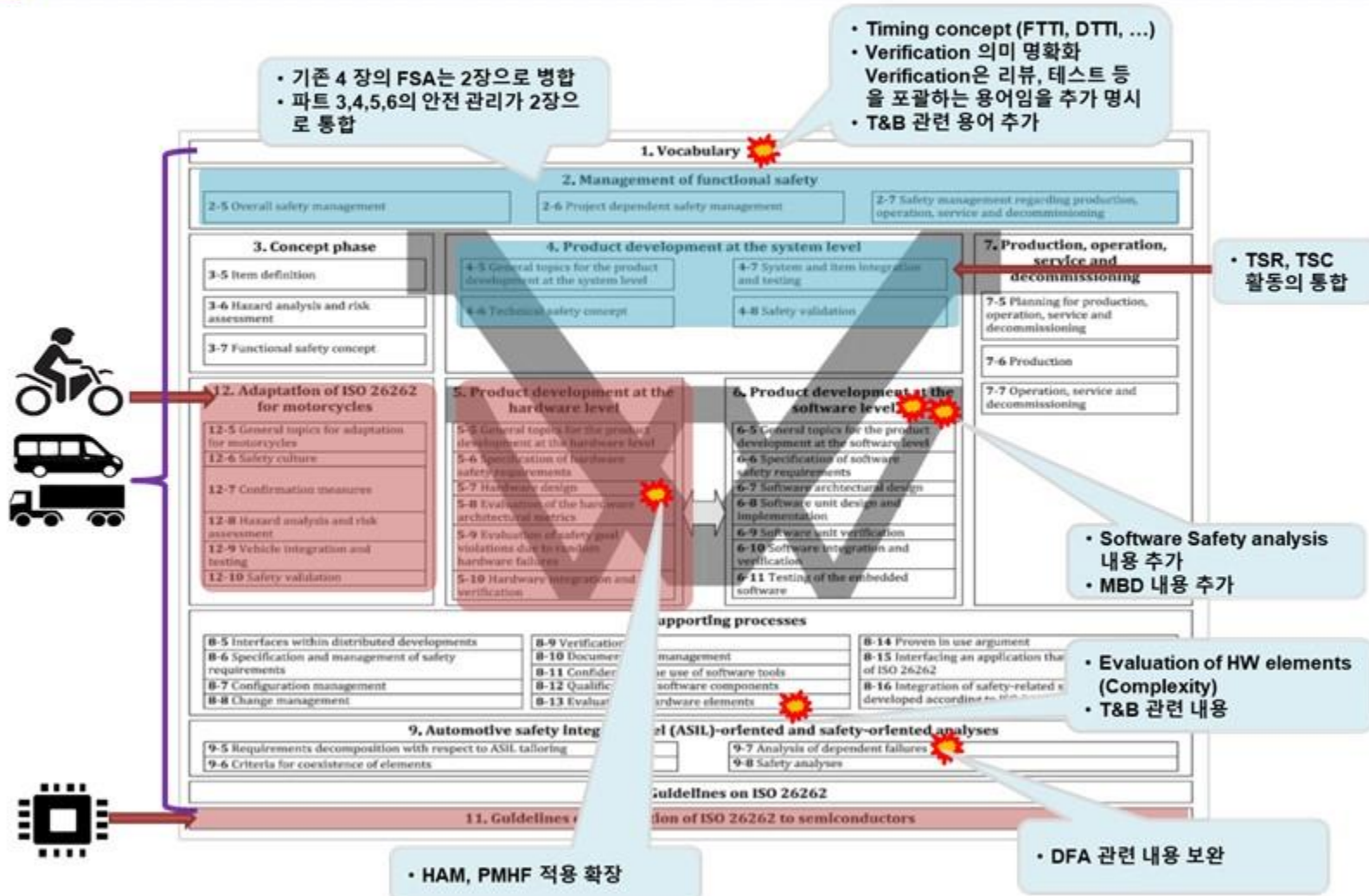
Hazardous event := Combination_(OS, Hazard)

Severity?
Exposure?
Controllability

Safety Goal and its ASIL of Item

Functional Safety Concept

II-1 Functional Safety & SOTIF (2/4)



II-1 Functional Safety & SOTIF (3/4)

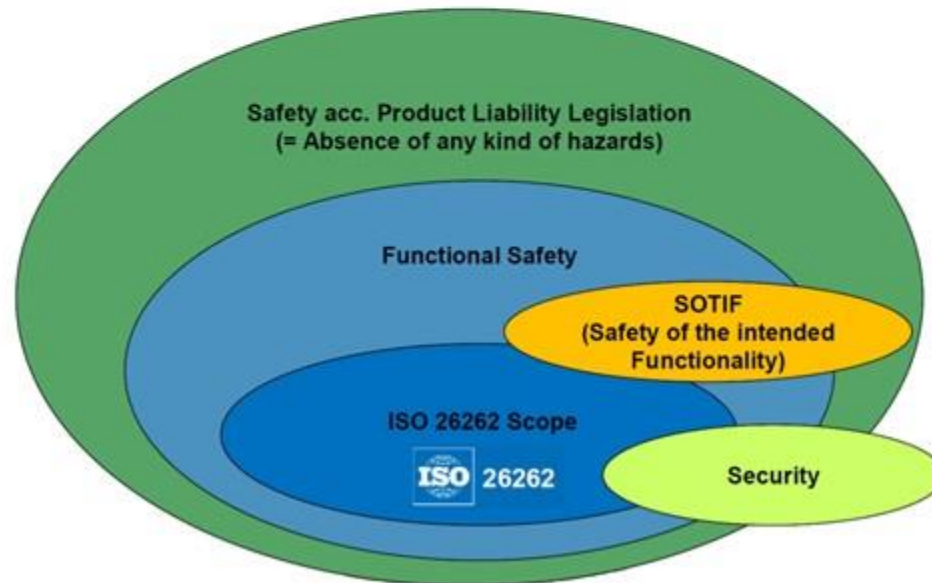
ISO 21448 SOTIF(Safety of the intended functionality)



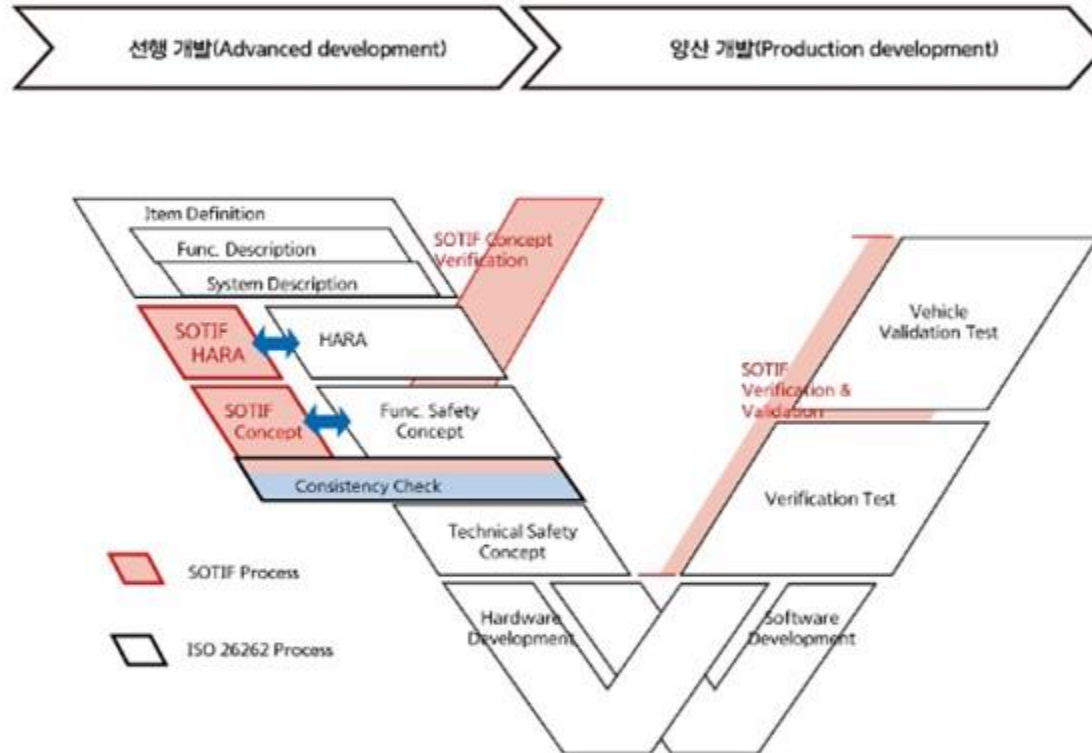
★ 진행 현황

- 총 10개의 ST(Sub Team) 운영중

ISO 26262 covers only a subset of safety



II-1 Functional Safety & SOTIF (4/4)



출처: Riccardo Manani
Intel Fellow, Internet of Things Group
Chief Functional Safety Technologist

<SOTIF Development Process Overview>

II-2 Cybersecurity (1/4)

ISO 21434 Cybersecurity engineering



ISO 21434 Cybersecurity engineering

PG 1	PG 2	PG 3	PG 4
Risk Management	Product Development	Operations, Maintenance and Other Processes	Process Overview and Interdependencies

II-2 Cybersecurity (2/4)



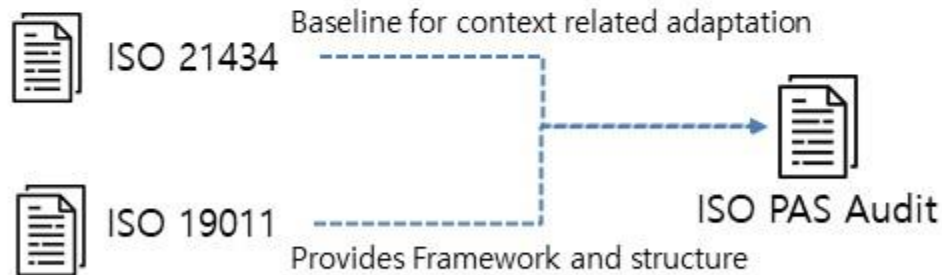
1. Scope									
2. Normative references									
3. Terms and abbreviations									
4. General considerations									
5. Overall cybersecurity management									
5.4.1 Cybersecurity governance	5.4.2 Cybersecurity culture	5.4.3 Cybersecurity risk management	5.4.4 Organizational cybersecurity audit	5.4.5 Information sharing	5.4.6 Management systems	5.4.7 Tool management	5.4.8 Information security management		
6. Project dependent cybersecurity management									
6.4.1 Cybersecurity responsibilities & their assignment	6.4.2 Cybersecurity planning	6.4.3 Tailoring of the cybersecurity activities	6.4.4 Reuse	6.4.5 Component out of context	6.4.6 Off the-shelf component	6.4.7 Cybersecurity case	6.4.8 Cybersecurity assessment	6.4.9 Release for post-development	
7. Continuous cybersecurity activities									
7.3 Cybersecurity monitoring		7.4 Cybersecurity event assessment		7.5 Vulnerability analysis		7.6 Vulnerability management			
8. Risk assessment methods									
8.3 Asset identification	8.4 Threat scenario identification	8.5 Impact rating	8.6 Attack path analysis	8.7 Attack feasibility rating	8.8 Risk determination	8.9 Risk treatment decision			
Concept phase			Product development phases				Post-development phases		
9. Concept phase			10. Product development				11. Cybersecurity validation		
9.3 Item definition			10.4.1 Refinement of cybersecurity requirements and architectural design						
9.4 Cybersecurity goals			10.4.2 Integration and verification						
9.5 Cybersecurity concept			10.4.3 Specific requirements for software development						
							12. Production		
							13. Operations and maintenance		
							13.3 Cybersecurity incident response		13.4 Updates
							14. Decommissioning		
15. Distributed cybersecurity activities									
15.4.1 Demonstration and evaluation of supplier capability			15.4.2 Request for quotation			15.4.3 Alignment of responsibilities			
Annexes A-J (Informative)									

II-2 Cybersecurity (3/4)

ISO NP 5112 Guidelines for auditing cybersecurity engineering



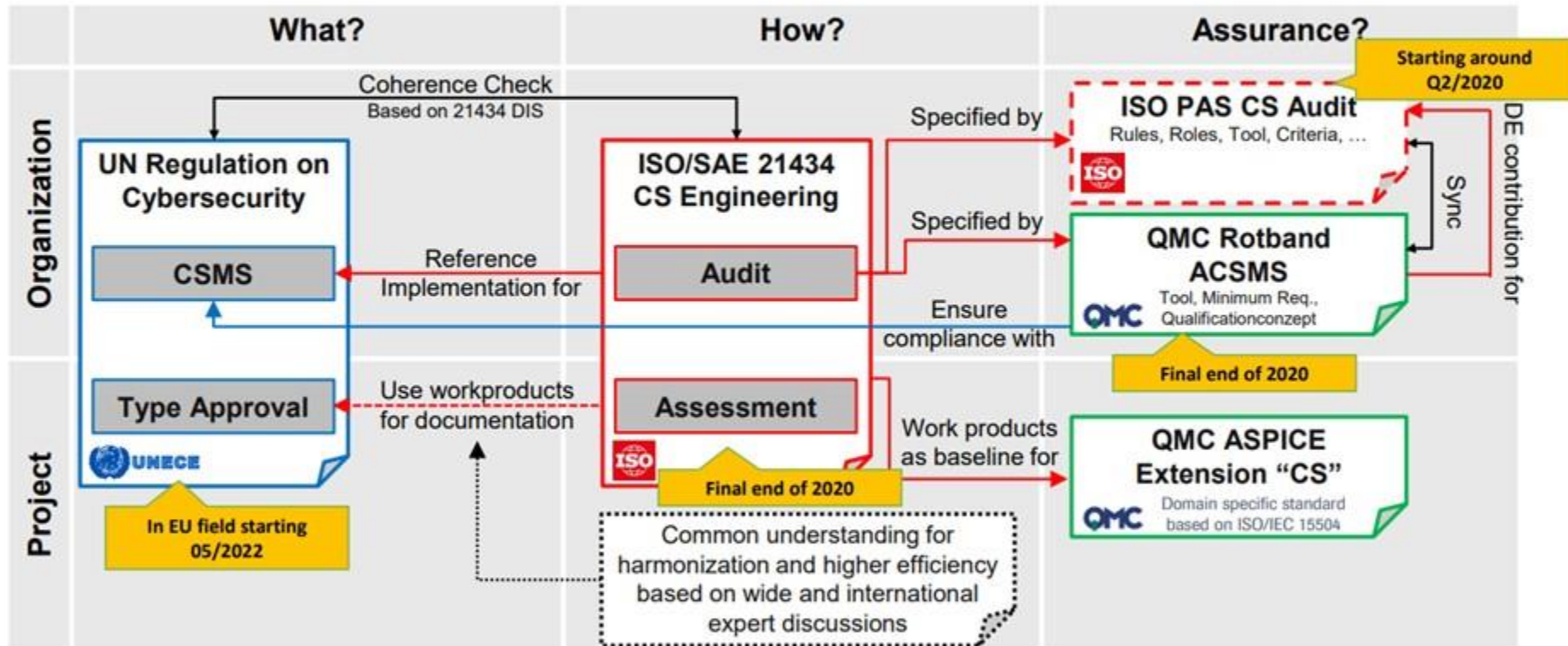
★ 문서 구조



★ 개발 일정

- NP vote: ~5/6
- Kick-off meeting: 5/28
- WD: 7/31
- CD ballot: 2021/01/29
- Publication: 2021/05/31

II-2 Cybersecurity (4/4)



II-3 Software Update Engineering

ISO 24089 Software update engineering



★ 진행 현황

- Terminology TF, Restructuring TF

1. Scope			
2. Normative references			
3. Terms and definitions			
4. Management activities			
5. Design and development of infrastructure for software update	6. Design and development of update-capable vehicles and components	7. Package development	8. Operations

<ISO 24089 개요>

ISO/TC 22 신규 프로젝트

ISO TR 4804 "Road vehicles –

Safety and cybersecurity for automated driving systems –

Design, verification and validation methods"

III-1 TC 22 신규 프로젝트 - TR 4804

- This is regarded as a long term ISO standardization activity for Safety and Cybersecurity for Automated Driving Systems
- The intl. working group shall be formed now and jointly proceed down the standardization road.
- Standardization of the state-of-the-art shall take place in parallel with the product developments of the contributing expert's companies.
- This activity is regarded as a application specific standardization for automated driving based on generic underlying standards like ISO 26262 (functional safety), ISO 21448 (SOTIF) , ISO 21434(automotive cybersecurity) and others, see ISO DTR 4609 (Road vehicles — Report on standardization prospective for automated vehicles (RoSPAV))

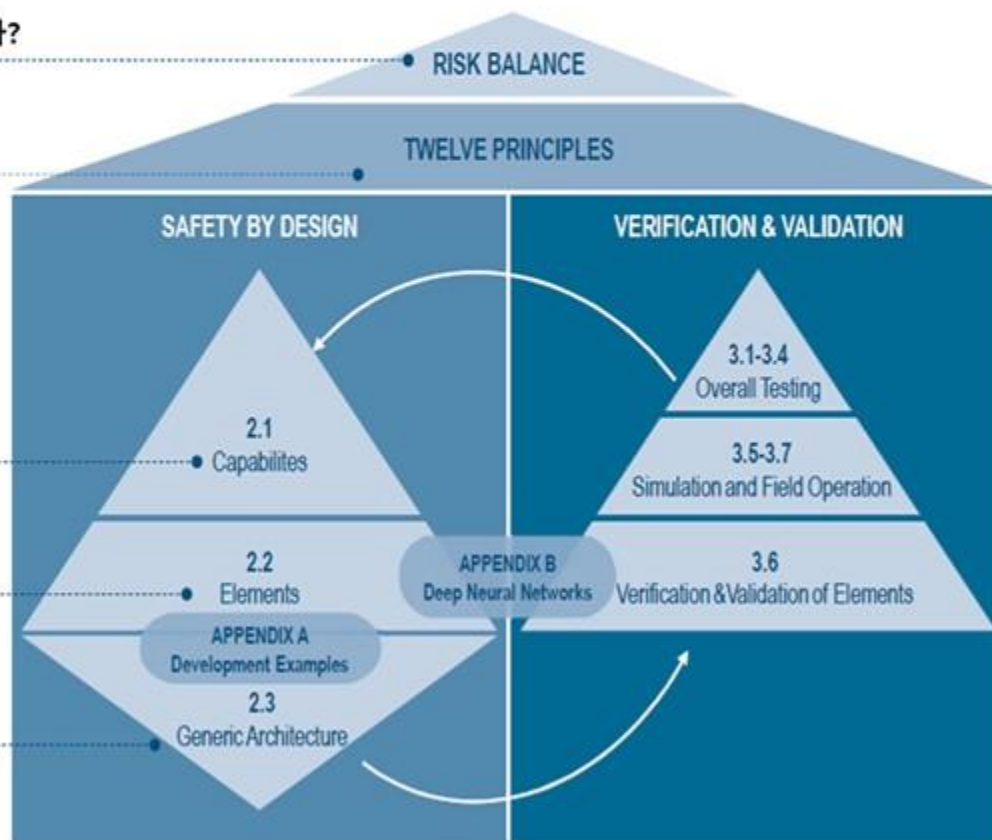
Focused on
"Automated Driving System"
(Level 3, 4 System)



III-2 TR 4804 구조

THINKING SAFETY FROM THE TOP DOWN – FROM RISK BALANCE TO IMPLEMENTATION

- ① L3/L4 시스템이 얼마나 안전해야 하나?
- ② 안전목표를 달성하기 위해 필요한 것은 무엇인가?
- ③ 위의 관점을 달성하기 위한 어떤 개념이 필요한가?
- ④ 개념을 구현하기 위해 어떤 Block이 필요한가?
- ⑤ 어떻게 이런 Block을 기반으로 일반적인 아키텍처 설계를 할 것인가?



III-3 Verification & Validation - Summary of the test strategy

Summary of the Test Strategy					
	SIL/SW Repro.	HIL/HW Repro.	DiL	Proving Ground	Open Road
Components					
Sensor Fusion, Localization, Perception					
System without Sensors, Prediction (Drive Planning)					
Motion Control, Egomotion					
HMI, User State Detect., ADS Mode Manager					
Entire System					

- Technical Aspects of SOTIF
- Human factors aspects of SOTIF
- Functional safety
- Security penetration testing
- Validation of virtual platforms



감사합니다.