TOWARDS A HOLISTIC ASSURANCE METHODOLOGY:
FROM COMPONENT TO INFORMATION ASSURANCE

Arash Khabbaz Saberi, Andre Smulders, Johan J. Lukkien

TNO innovation for life

AUTOMATION LEVELS

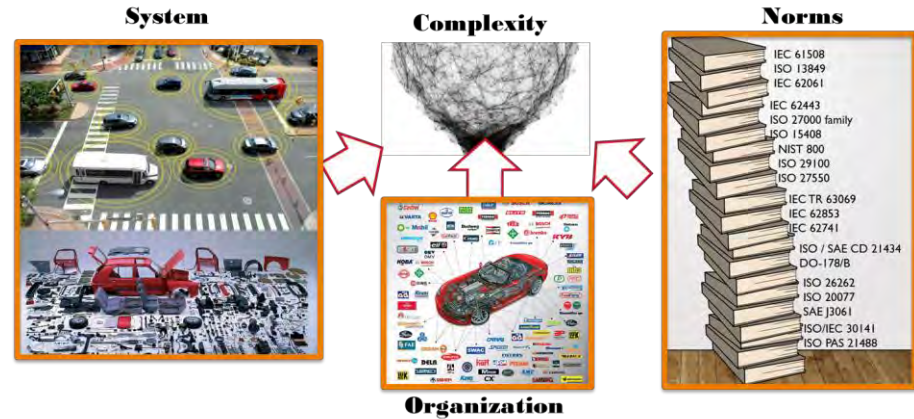| Level 0	Level 1	Level 2	Level 3	Level 4/5
				SoS and AI
			Smart Systems	**Smart Systems**
		software	software	software
	firmware	firmware	firmware	firmware
physical components	physical components	physical components	physical components	physical components

ASSURANCE CHALLENGES

› Harmonizing safety and security assurance

› Translating traffic level risks into vehicle level risk

› Segmentation of vehicle architecture from safety and security view

› Complexity of assurance space from three aspects (see Figure 2): Connectivity of vehicle to the traffic system, Long supply chain, Increasing number of norms and standards.

System

Complexity

Norms

IEC 61508
ISO 13849
IEC 62061

IEC 62443
ISO 27000 family
ISO 15408
NIST 800
ISO 29100
ISO 27550

IEC TR 63069
IEC 62853
IEC 62741

ISO / SAE CD 21434
DO-178/B

ISO 26262
ISO 20077
SAE J3061
ISO/IEC 30141
ISO PAS 21488

Organization

ASSURANCE TREND

Level 0	Level 1	Level 2	Level 3	Level 4/5
				Information Assurance
			Function Assurance	**Function Assurance**
		E/E Assurance	**E/E Assurance**	**E/E Assurance**
	Mechanical Assurance	**Mechanical Assurance**	**Mechanical Assurance**	**Mechanical Assurance**
Quality System	**Quality System**	**Quality System**	**Quality System**	**Quality System**

TNO innovation for life

TOWARDS INFORMATION ASSURANCE

› Already Existing
  › Quality System (ISO9001 or ISO/TS 16949)
  › Mechanical Assurance (Type approval (EU) 2018/858)
  › E/E Assurance (safety in ISO 26262 and security in ISO/SAE 21434)

Level 0	Level 1	Level 2	Level 3	Level 4/5
				Information Assurance
			Function Assurance	Function Assurance
		E/E Assurance	E/E Assurance	E/E Assurance
	Mechanical Assurance	Mechanical Assurance	Mechanical Assurance	Mechanical Assurance
Quality System	Quality System	Quality System	Quality System	Quality System

TOWARDS INFORMATION ASSURANCE

› Already Existing
  › Quality System (ISO9001 or ISO/TS 16949)
  › Mechanical Assurance (Type approval (EU) 2018/858)
  › E/E Assurance (safety in ISO 26262 and security in ISO/SAE 21434)
› In Preparation
  › ISO/PAS 21448: (SOTIF)

TOWARDS INFORMATION ASSURANCE

› Already Existing
  › Quality System (ISO9001 or ISO/TS 16949)
  › Mechanical Assurance (Type approval (EU) 2018/858)
  › E/E Assurance (safety in ISO 26262 and security in ISO/SAE 21434)
› In Preparation
  › ISO/PAS 21448: (SOTIF)
› Future
  › Information assurance
    › Quantitate risk assessment
    › SoS Architecture
    › Integrated Cybersecurity and Functional Safety
      › Data trustworthiness, validity, and integrity
    › Method for assurance case analysis

Level 0	Level 1	Level 2	Level 3	Level 4/5
				Information Assurance
			Function Assurance	Function Assurance
		E/E Assurance	E/E Assurance	E/E Assurance
	Mechanical Assurance	Mechanical Assurance	Mechanical Assurance	Mechanical Assurance
Quality System	Quality System	Quality System	Quality System	Quality System

SIMPLEXITY ROADMAP
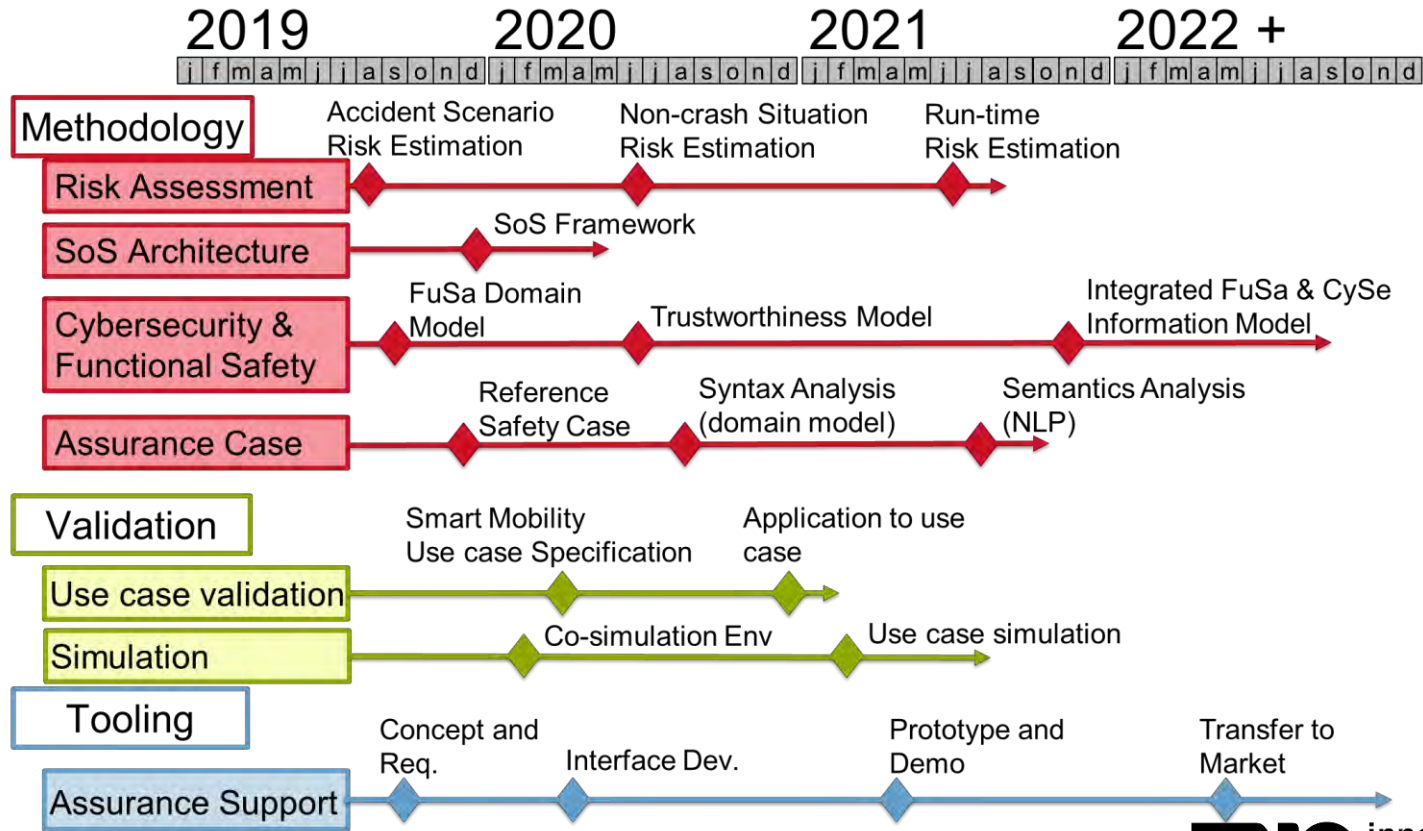
THANKS FOR YOUR ATTENTION

ARASH KHABBAZ SABERI

arash.khabbazsaberi@tno.nl