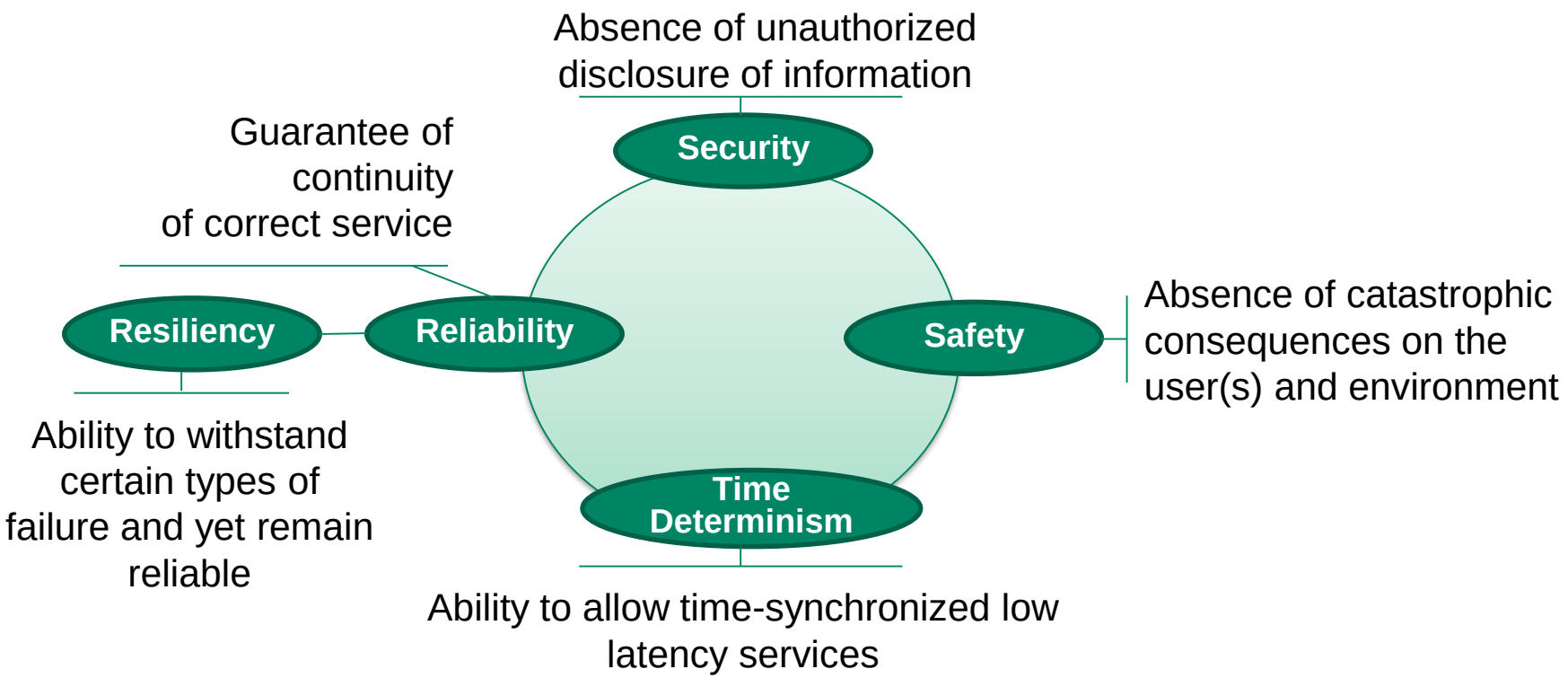
AN INTEGRATED APPROACH TO SAFETY AND SECURITY IN AUTONOMOUS SYSTEMS

RICCARDO MARIANI | VP, INDUSTRY SAFETY | DECEMBER 2nd, 2019

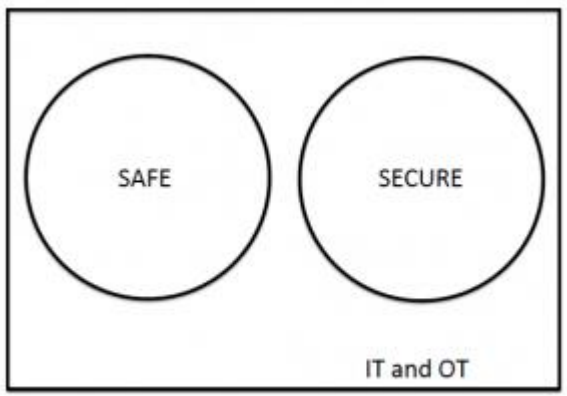
AUTONOMOUS SYSTEMS DEPENDABILITY

Definitions

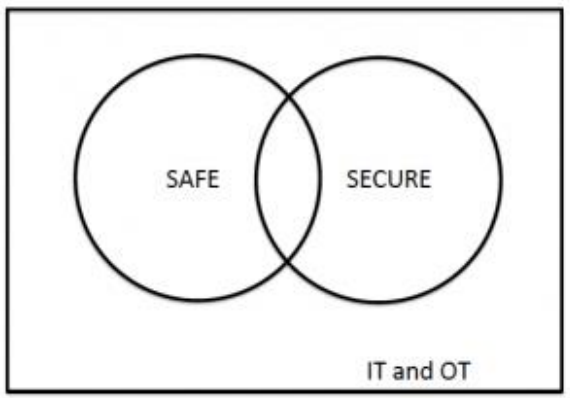


SAFETY AND (CYBER) SECURITY

From “The interaction between safety and security”, C.Hankin

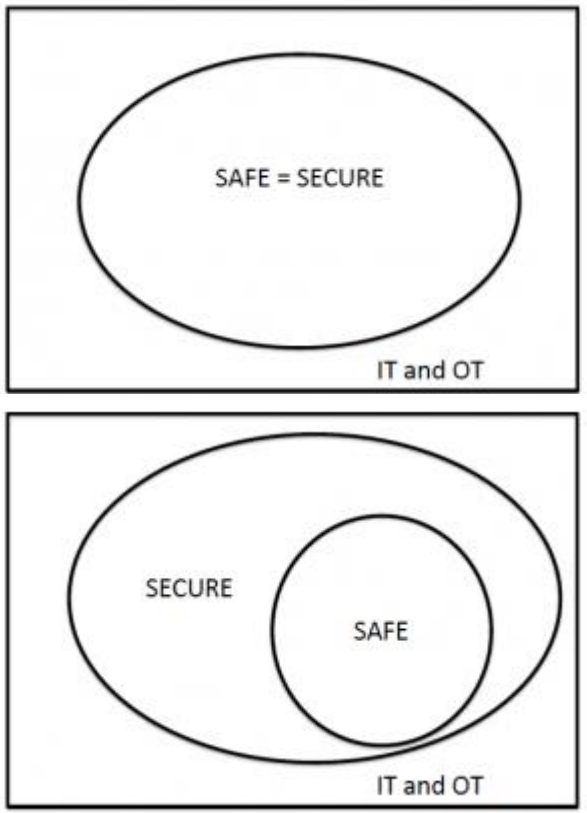


Today standards



Field experience

Goal



SAFETY

ISO 26262, ISO 21448, UL4600

ISO 26262

- Well consolidated family of standards addressing functional safety management, HW random and systematic failures
- Main issues:
  - AD complexity (multiple items combined, thousand of safety requirements) requires a more agile development flow.
  - no AD system architecture references.
  - current PMHF targets do not match with modern technologies / components.
  - ISO 26262-6 is unaffordable / very challenging if applied to open source SW.
  - guidelines missing on how to apply ISO 26262 to Artificial Intelligence.

ISO 21448

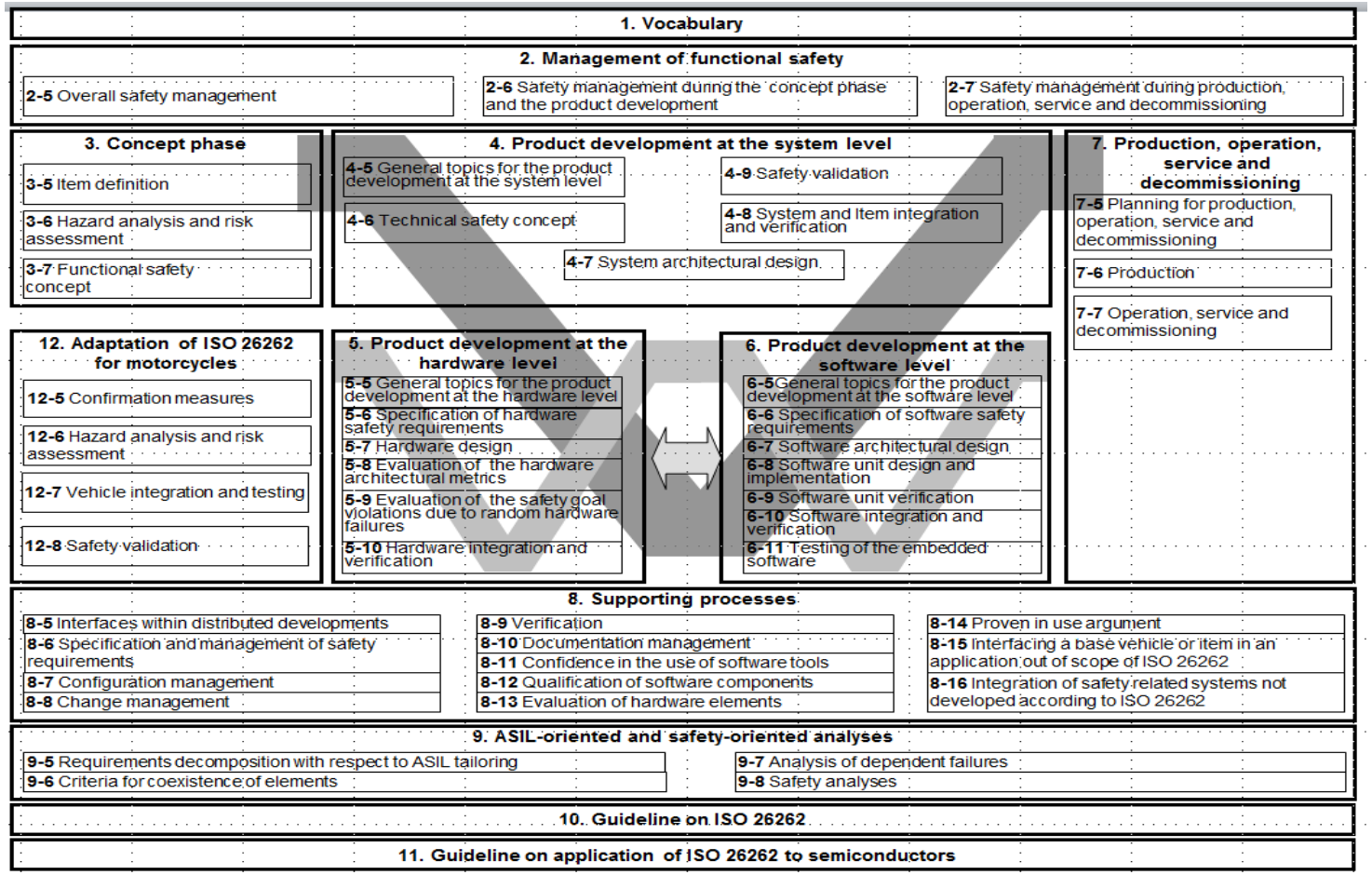
- New ongoing standard addressing:
  - the inability of the function to correctly comprehend the situation and operate safely
  - insufficient robustness of the function with respect to sensor input variations or diverse environmental conditions
- Main issues:
  - standard at today is too high level to produce consistent / interoperable industry practices
  - not (yet) clear which are the different requirements between AD levels (L2/L2+/L3/L4/L5)
  - some annexes (e.g. machine learning) require additional work

UL 4600

- A new standard that covers safety principles and processes for evaluating autonomous products
- Main issues:
  - it seems a not organic set of very prescriptive requirements
  - OEM/Tier1 involvement so far very limited
  - Potential overlaps with ISO 26262 and ISO 21448
  - Unclear how UL certification will work in the AD area

ISO 26262 LIFECYCLE

Source: ISO 26262 2nd edition



SECURITY

SAE J3061, ISO/SAE 21434

SAE J3061

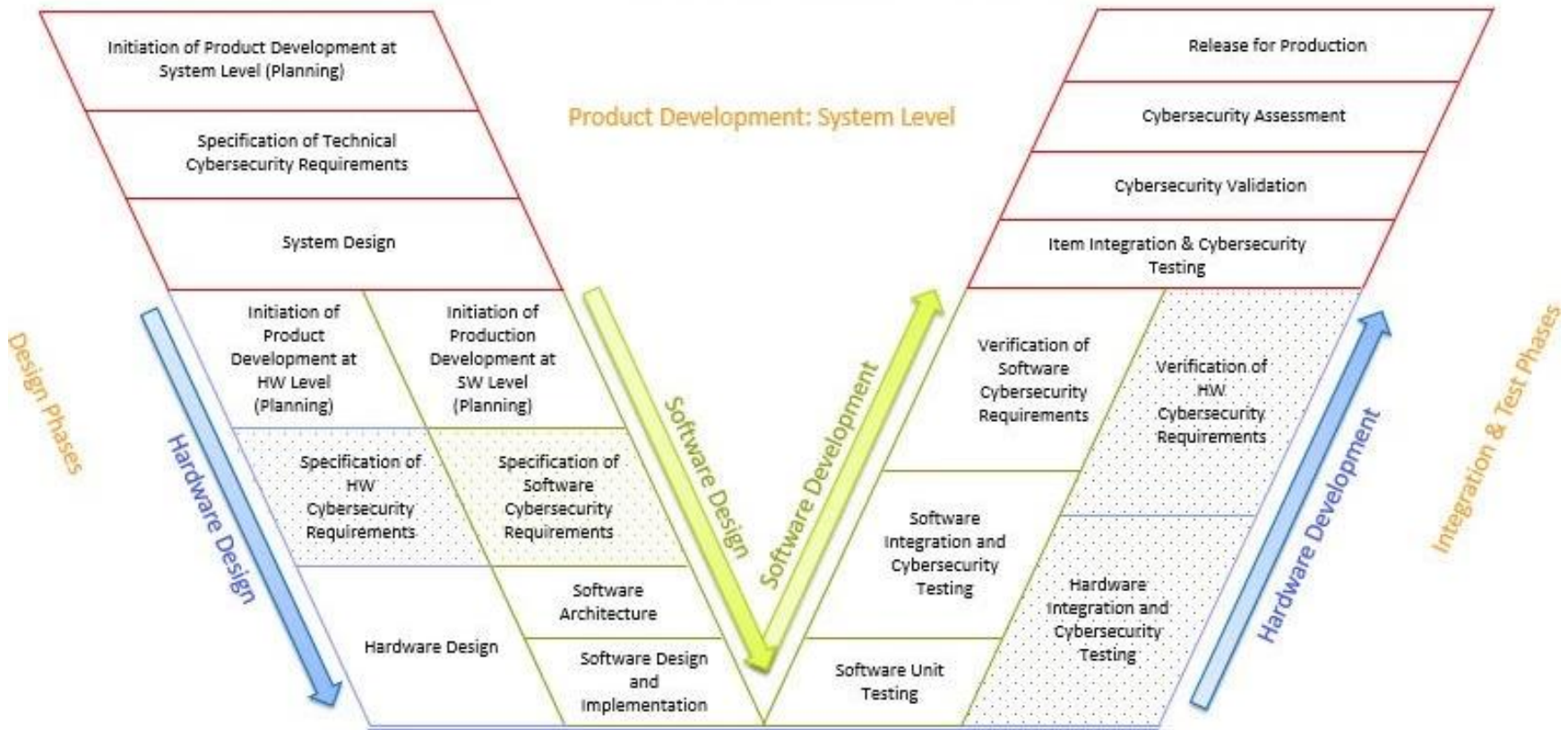
- Provides guidance on vehicle cybersecurity and was created based off of, and expanded on from, existing practices which are being implemented or reported in industry, government and conference papers.
- Main issues:
  - It is a collection of guidance's
  - It does not consider interaction with safety

ISO/SAE 21434

- New standard jointly developed by ISO and SAE:
  - Applicable to Road-vehicles.
  - Goal of reasonably secure vehicles and systems.
  - Automakers and Suppliers can use to show “due diligence”.
  - Focus on automotive cybersecurity engineering.
  - Based on current state-of-the-art for Cybersecurity Engineering
  - Risk-oriented approach
  - Management activities for Cybersecurity
  - Cybersecurity activities/processes for all phases of vehicle lifecycle
- Main issues:
  - It is high level
  - It does not consider interaction with safety

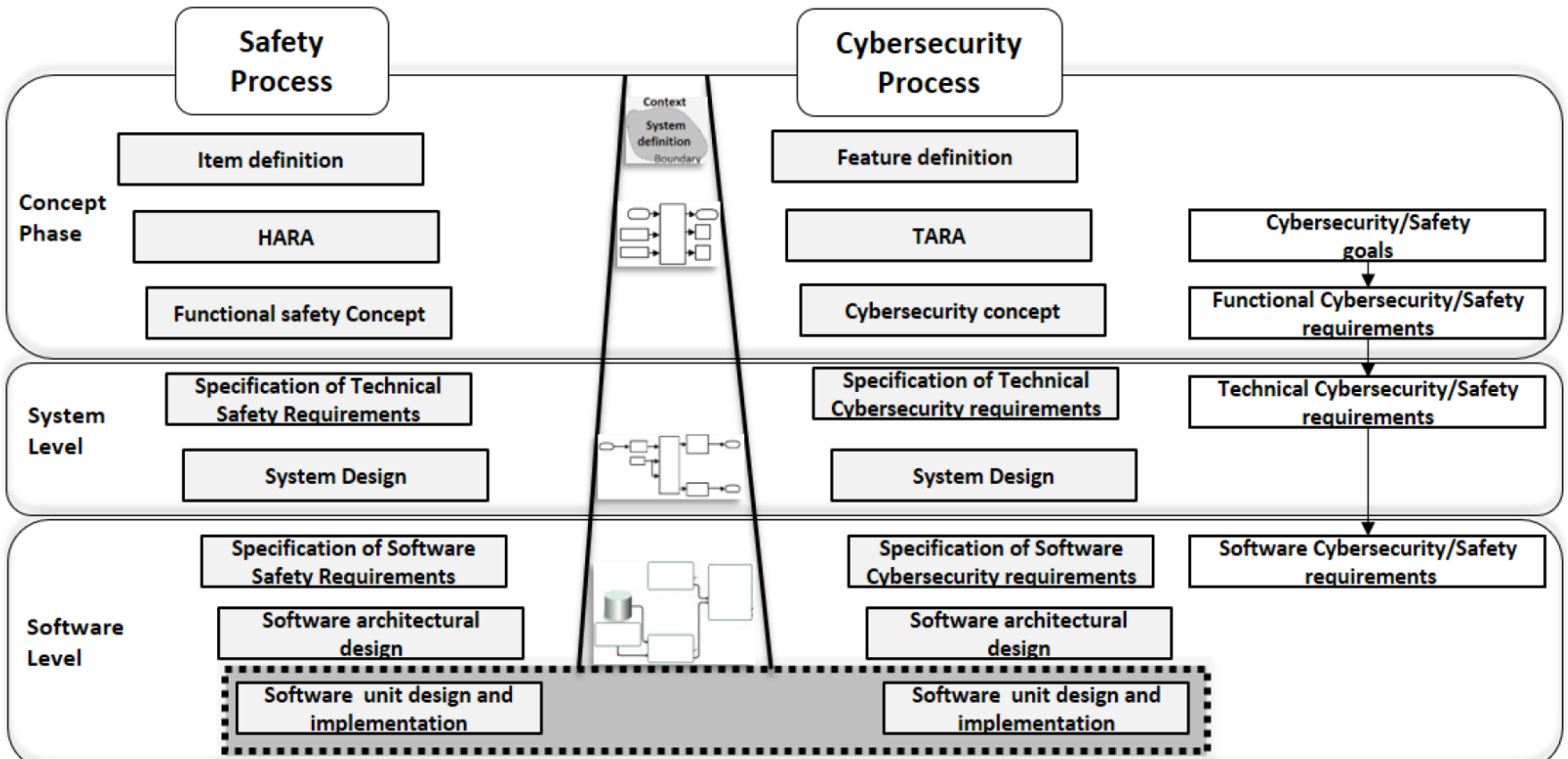
SAE J3061 LIFECYCLE

Source: SAE J3061



PROCESS COMPARISON

ISO 26262 vs SAE J3061



From paper “Towards Efficiently Checking Compliance Against Automotive Security and Safety Standards”

GAPS FOR AN INTEGRATED APPROACH

- Gaps to be addressed for an integrated safety-security approach:
  - Common structure/language to
    - perform HARA and TARA
    - describe safety and cybersecurity concepts
    - describe safety and cybersecurity requirements
    - perform safety and cybersecurity analyses
    - perform safety and cybersecurity verification
  - Requirements for Interactions between safety and cybersecurity
    - Safety affecting cybersecurity, and viceversa
    - Safety helping cybersecurity, and viceversa

NEW IEEE INITIATIVES

www.computer.org/communities/special-technical-communities/rsstdis

1st meeting in Bologna (Italy) on December 6th

P2846

P2851

P2846

Title: Formal Model for Safety Considerations in Automated Vehicle Decision Making

Sponsoring Society and Committee: IEEE Vehicular Technology Society/Intelligent Transportation Systems (VT/ITS)

Joint Sponsor: IEEE Computer Society Standards Activity Board Standards Committee

Scope: This standard defines formal rules-based mathematical model for automated vehicle decision making using discrete mathematics and logic. The model applies to the planning and decision-making functions of an SAE Level 3-5 automated vehicle. The model is formally verifiable, technology neutral, and parameterized to allow for regional customization by governments as desired. The standard applies to specified driving scenarios and cases. For example, some scenarios include highway driving and potentially full urban driving. The standard also describes a test methodology and tools necessary to perform verification of an automated vehicle to assess conformance with the standard. The proposed standard does not address the host vehicle navigation system implementing the logic or anything relating to perception, object detection, recognition, verification and/or classification, free space detection, etc.

P2851

Title: Exchange/Interoperability Format for Safety Analysis and Safety Verification of IP, SoC and Mixed Signal Ics

Sponsoring Society and Committee: IEEE Computer Society/Design Automation (C/DA)

Joint Sponsor: IEEE Computer Society Standards Activity Board Standards Committee

Scope: This standard defines a data format with which results of safety analyses (such as FMEA, FMEDA, FMECA, FTA) and related safety verification activities - such as fault injection - executed for IPs, SoCs and mixed signal ICs can be exchanged and made available to system integrators. The format will define languages, data fields and parameters with which the result of those analyses and verification activities can be represented, in a technology independent way. Goal of the standard is to provide a common ground for EDA, SoC and IP vendors in needs of developing tools, SoC and IP for safety critical applications


NVIDIA