FOR ENERGY EFFICIENT INNOVATIONS

THINK ON.

www.onsemi.com

Introduction to the IEEE P2851 working group

Exchange/Interoperability Format for Safety Analysis and Safety Verification

Chanthachith Souvanthong

Corporate Functional Safety Manager

Materials prepared in collaboration with:

Riccardo Marianni and Jyotika Athavale from Nvidia

IEEE P2851

Overview

IEEE COMPUTER SOCIETY

IEEE

About P2851

- IEEE P2851 is about “Exchange/Interoperability Format for Safety Analysis and Safety Verification”.
- Its initial scope was IPs and ICs but its scope has been extended to items, systems and SW as well.
- Artificial Intelligence is also a key part of the activity.
- Leadership team:
  - Chair: Election on going (Formally Riccardo Mariani, NVIDIA)
  - Vice Chair: Election on going (Nir Maor, QUALCOMM)
  - Secretary: Election on going (Jyotika Athavale, NVIDIA)
  - IEEE CS DASC Chair: Dennis Brophy, Mentor *(P2851 will move to FSSC)*
  - IEEE Program Manager: Jonathan Goldberg and Vanessa Lalitte, IEEE-SA
- As of today, 34 companies (IP/IC providers, EDA vendors, Tier1s and OEMs) are members with 70+ active individuals.
- The P2851 is already referenced by ISO/TR 4804.

P2851 members

P2851 and IEEE FSSC

- IEEE Computer Society decided to create an overall container (named “FSSC”) for everything related to functional safety.
- The scope is:

  The Functional Safety Standards Committee (FSSC) is responsible for functional safety-related standards in the IEEE where functional safety means the part of the overall safety of a system or piece of equipment that depends on a system or equipment operating correctly in response to its inputs. The FSSC is focused on architectures, methodologies, tools addressing functional safety and other safety-related aspects of the intended functionality at the different levels of abstraction (system of systems, systems, hardware or software component) and across application fields such as automotive, industrial, avionics, high-performance computing. It also covers relationships of functional safety with contiguous domains such as system safety, cybersecurity, reliability, real-time interactions, and artificial intelligence.

- Status:
  - approved by C/SAB (Standards Activities Board) and CS BoG (Board of Governors),
  - approved by IEEE SA AudCom, SASB and BoG
  - Starting the activity in April 2021
  - P2851 will move from DASC (Dependable, Automotive and Secure Computing) to FSSC.
  - FSSC will be also the co-sponsor of P2846

P2851 activities and roadmap

- 6 subgroups: Automotive FuSa, Artificial Intelligence, Avionics, Security, Industrial/Medical/Robotics, SOTIF
- Roadmap
  - Within April 2021
    - Publication of a white paper based on the first version of “landscape document”, describing lifecycle activities and related methodologies and tools needed
    - Partitioning of P2851 in sub-standards (P2851.0, P2851.1 etc.) to address different levels / use cases
  - Within end of 2021
    - first draft of the standard, incorporating outcomes of Accellera FSWG
  - Within end of 2022
    - final version of the standard

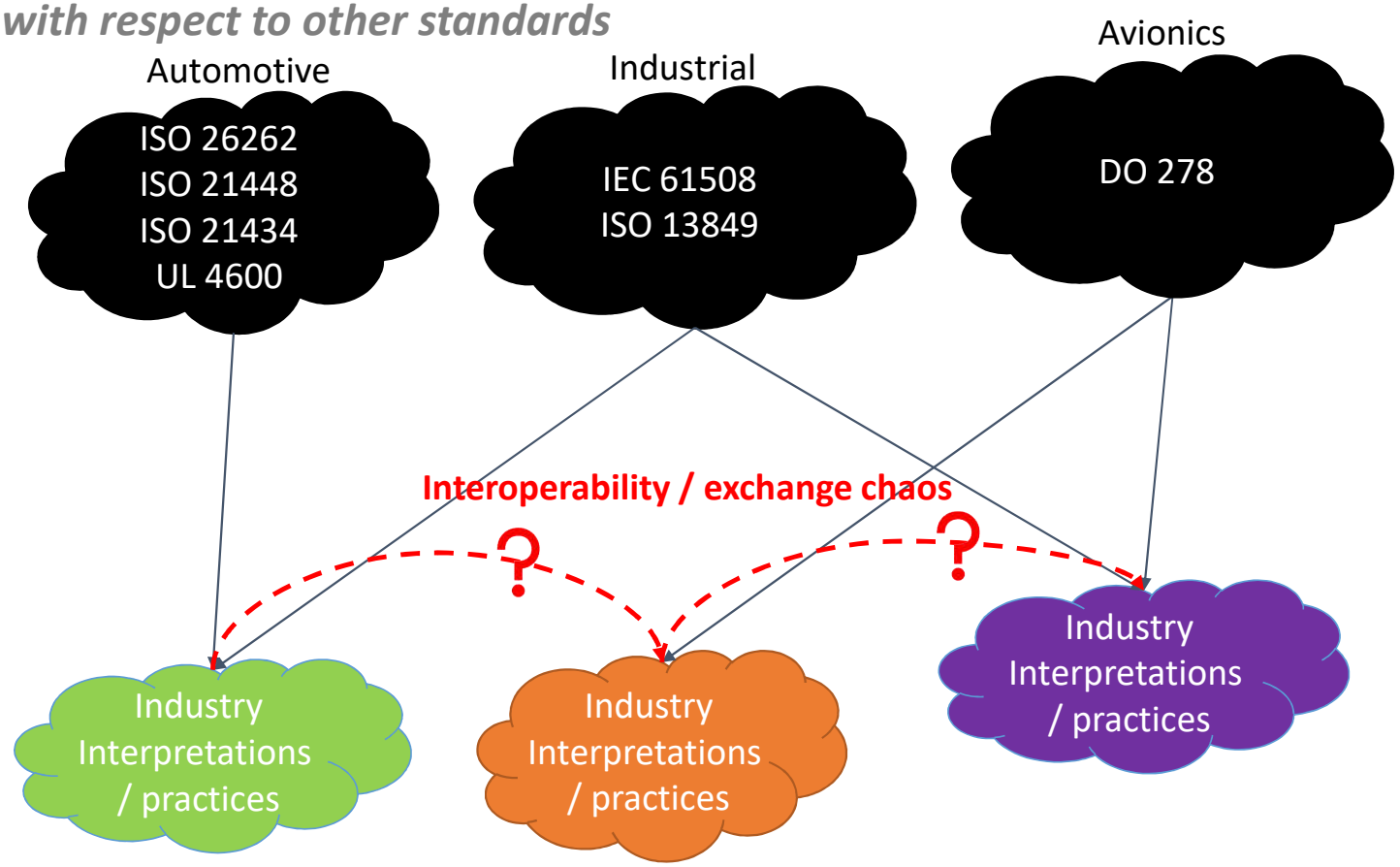
Slide 6

CS1 white paper positioned as based standard

Chanthachith Souvanthong; 24/03/2021

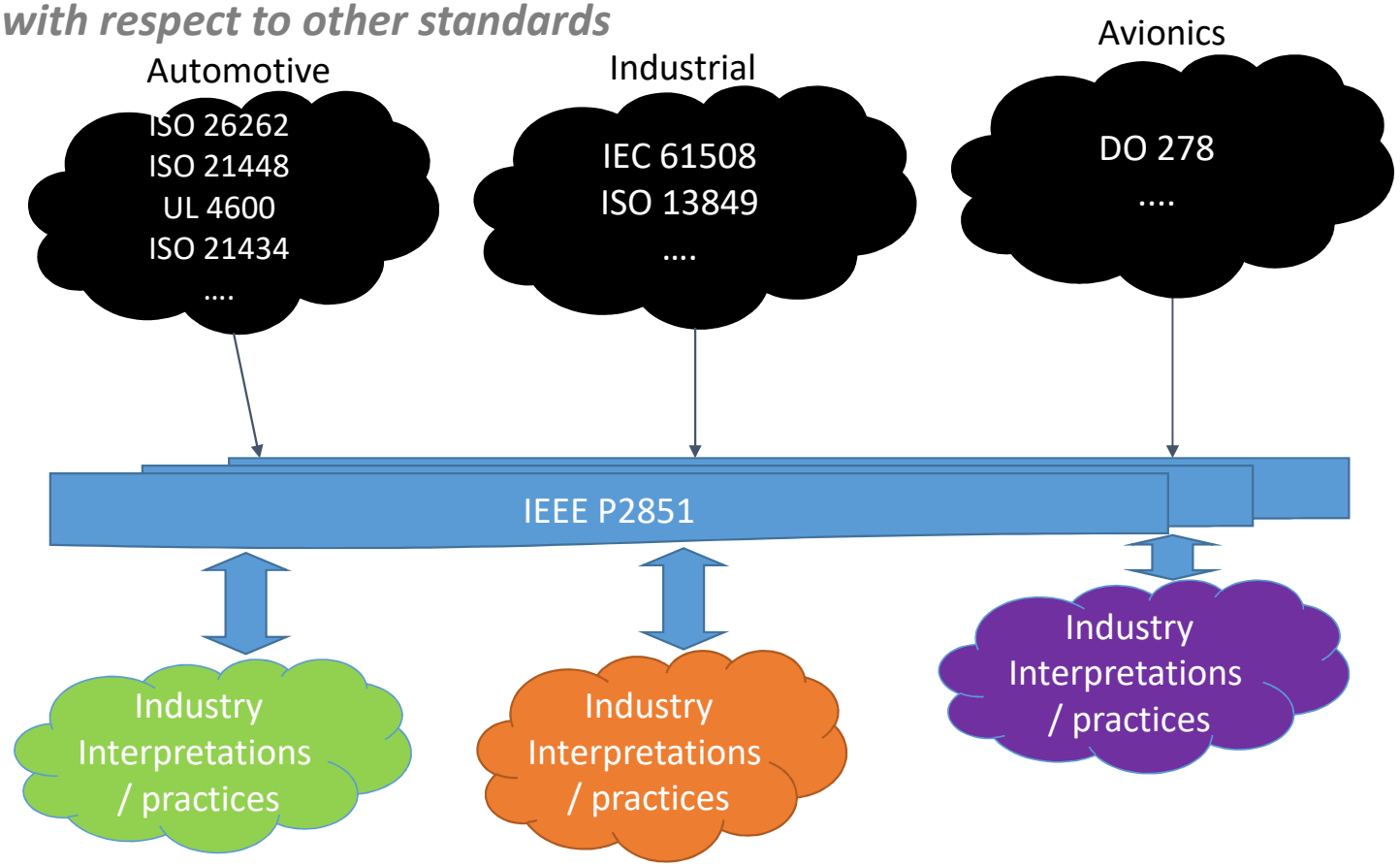
P2851 highlights

Position with respect to other standards



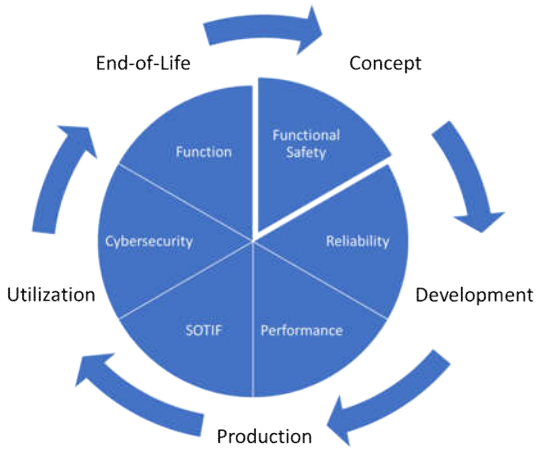
P2851 highlights

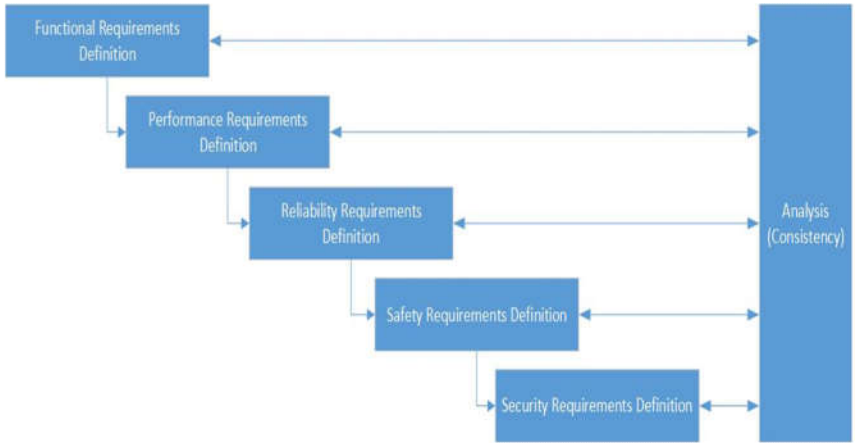
Position with respect to other standards



P2851 highlights

Product dependability lifecycle / Dependability lifecycle model





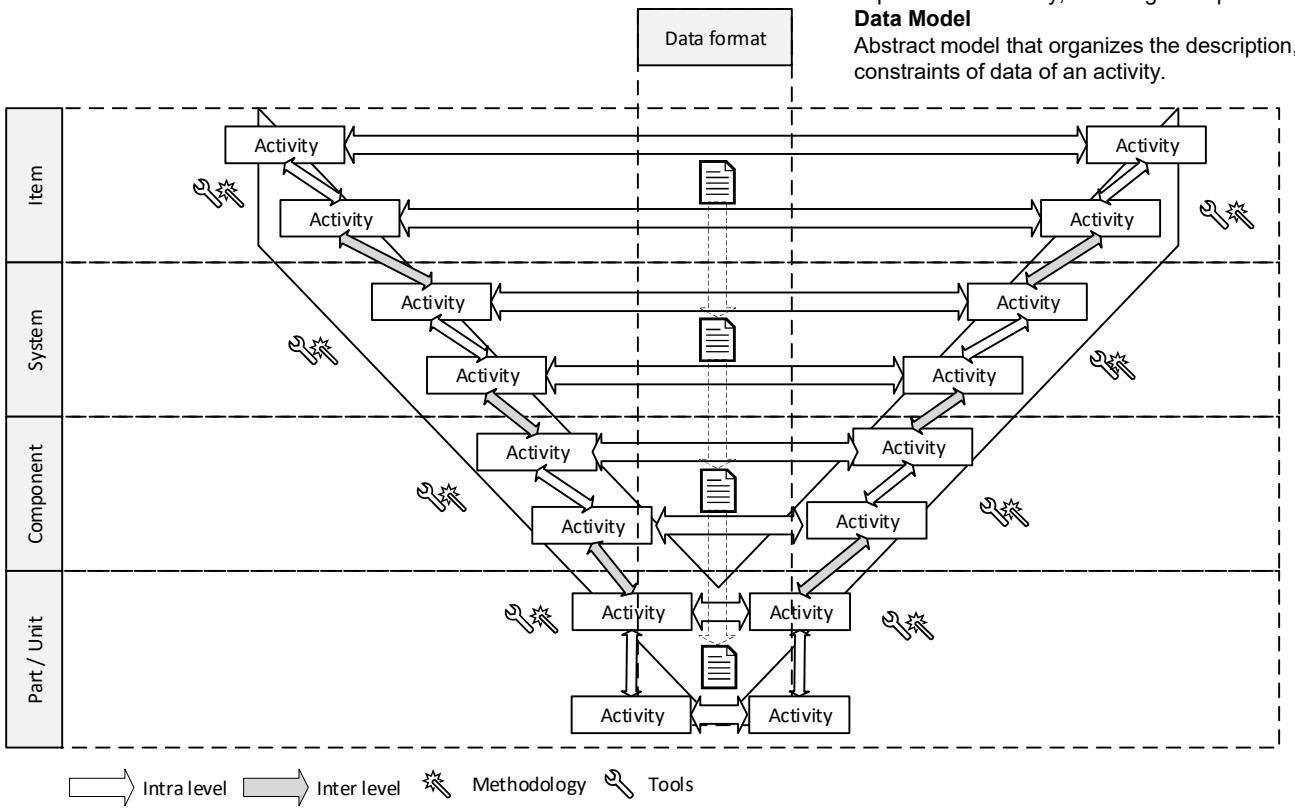
P2851 highlights

Landscape

Description Language
Language used to describe the framework, syntax and behavior of an activity. It can comprehend a data model.

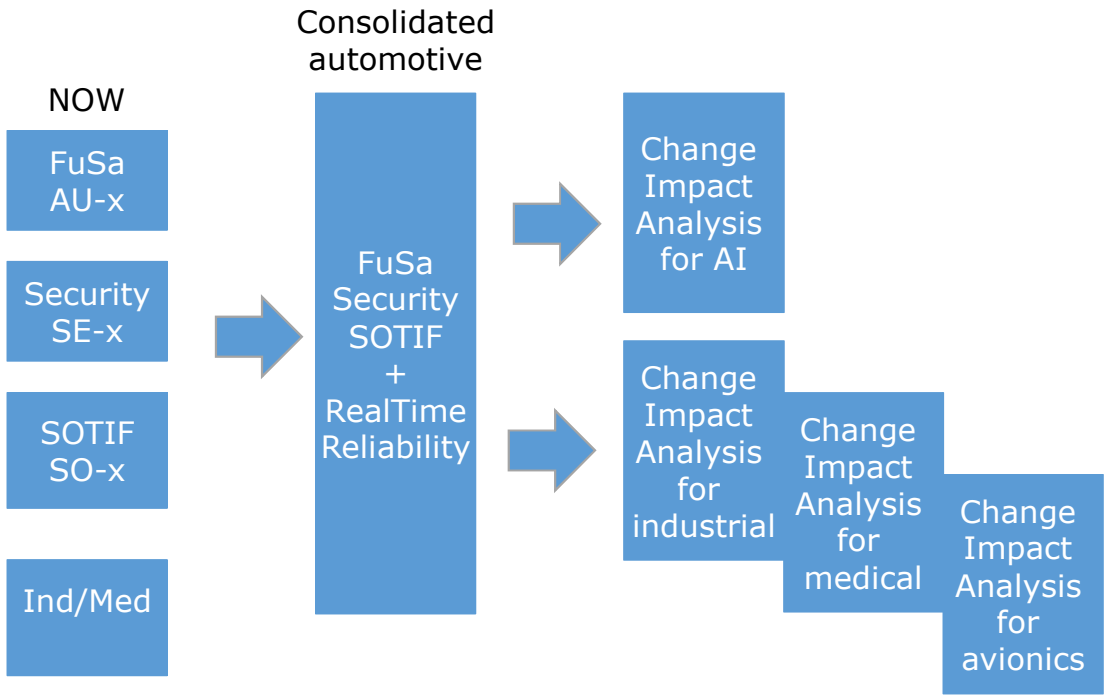
Methodology
Best known methods, guidelines and principles describing the detailed steps needed to implement an activity, including examples.

Data Model
Abstract model that organizes the description, the semantics, and consistency constraints of data of an activity.



P2851 highlights

Use cases



P2851 highlights

Needs: Description languages, methodologies, databases (excerpt)

Description Language
Language used to describe the framework, syntax and behavior of an activity. It can comprehend a data model.
Methodology
Best known methods, guidelines and principles describing the detailed steps needed to implement an activity, including examples.
Data Model
Abstract model that organizes the description, the semantics, and consistency constraints of data of an activity.

- DESCRIPTION LANGUAGES (DL)
  - Safety Plan & Safety Case DL
  - Confirmation Measures DL
  - External Measures DL
  - Assumptions of Use DL
  - Base Failure Rate (BFR) DL
  - Etc…
- METHODOLOGIES (ME)
  - Requirements evaluation ME
  - Vulnerability Factors ME
  - Dependent Failure Analysis ME
  - ASIL decomposition ME
  - Non-deterministic behavior analysis ME
  - Etc…
- DATABASES (DB)
  - Use environment DB
  - External measures DB
  - Severity, Controllability, Exposure DB
  - Safety mechanisms DB
  - AI training data DB
  - Etc..