The Importance of Interoperability in Functional Safety Standards

Riccardo Mariani, NVIDIA
Nir Maor, Qualcomm
Jyotika Athavale, NVIDIA
Kevin Gay, Aurora

The increase in standardization activities for automated vehicles is creating interoperability and information-exchange challenges for methodologies, models, and architectures. IEEE is addressing these issues through two standardization projects in functional safety: P2846 and P2851.

In the past few years, there has been a flourish of standardization activities related to functional safety, for example, in the case of automated vehicles (AVs). These standards, published by a few development organizations, such as IEEE, the International Organization for Standardization (ISO), the International Electrotechnical Commission (IEC), and UL, have provided requirements for specification, development, and testing of safety-critical elements at different levels [vehicle, system, software (SW), hardware, and integrated circuits (ICs)].

However, these requirements typically are very general, and so the resulting detailed implementation (in terms of methodologies, models, and architectures) can vary to the point that exchanging and combining the work products across the supply chain becomes extremely difficult. For example, a general requirement to provide a failure modes and effects analysis (FMEA) for an IC could cause, in the absence of specific guidelines, different silicon providers to produce disparate FMEAs

Digital Object Identifier 10.1109/MC.2021.3050453
Date of current version: 12 March 2021

with varying levels of abstractions and different assumptions. The deviations could be so large that the user of those FMEAs [the Tier 1 or original equipment manufacturer (OEM)] could expend significant effort to combine them for the system-level FMEA. Similarly, a general requirement to specify a safe-driving policy for automated driving could cause, in the absence of specific models, various OEMs or Tier 1s to produce implementations with such large differences that interoperability and verifiability versus common criteria (such as regulations) could be difficult or even impossible to achieve.

This challenge is becoming so critical that, in January 2020, the IEEE Computer Society (CS) decided to start a couple of standardization activities to address specific aspects related to the interoperability of functional safety standards: IEEE P2846[1] (sponsored by the IEEE Vehicular Technology Society and cosponsored by the CS) and P2851[2] (sponsored by the CS). The following paragraphs provide a status on the activity of the two projects after a year of development.

IEEE P2846

Reasonable and foreseeable assumptions play a critical role in the safety-related models used in automated driving systems (ADSs); however, the current body of industry consensus standards does not address how they are identified or establish a minimum set that AV developers should utilize. With that in mind, IEEE P2846 was created with the goal of identifying the minimum set of reasonable assumptions used in foreseeable scenarios to be considered for road vehicles in the development of safety-related models. While the specific values of the assumptions used in an ADS may be specified by regulation or selected by the ADS developer, the minimum set used within safety-related models is common to all ADS developers, regardless of what model is being used.

The IEEE P2846 Working Group (WG) is currently composed of 30 member organizations that encompass government agencies, research institutes, AV developers, OEMs, and Tier 1 suppliers. The WG has representatives from all over the globe, including Europe, the United States, Israel, Japan, and China, and it is led by Intel (chair), Waymo (co-chair), and Aurora (secretary).

In the past few years, there has been a flourish of standardization activities related to functional safety, for example, in the case of automated vehicles.

While the COVID-19 pandemic has impacted the WG's ability to meet in person, overall the group has made great strides in developing this standard during these challenging times. Over the past year, the WG utilized a set of five task forces operating in parallel to develop specific sections of the draft standard, which were assembled to create the draft standard. The WG also dedicated an entire week in November to virtual meetings to review and resolve hundreds of comments on the first complete draft standard submitted by the member entities.

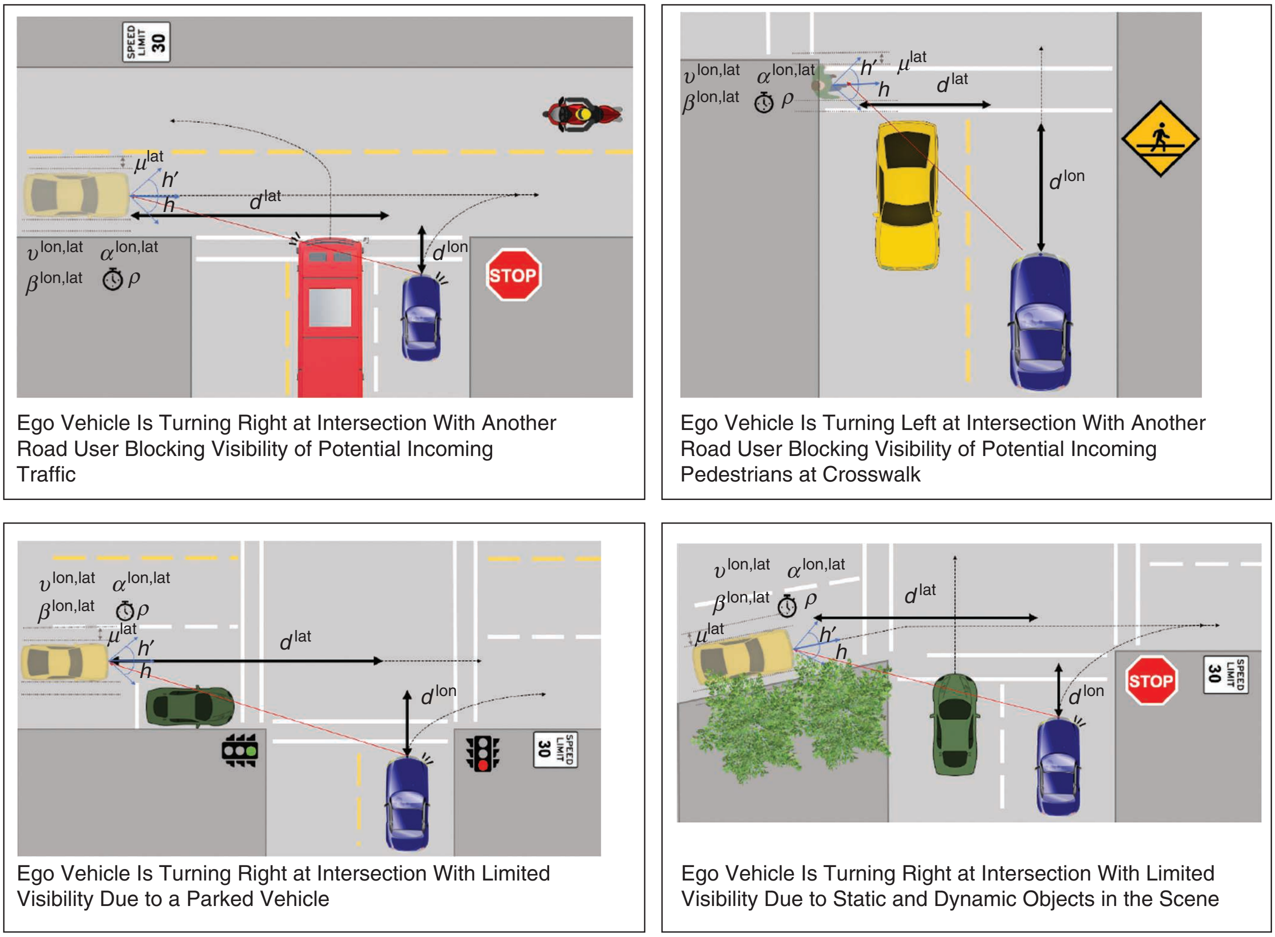
The core content produced by the task forces that currently comprises the draft standard is organized into three major sections. First, the "Scenarios and Assumptions" section identifies a set of scenarios covering safety-relevant driving situations that an AV may encounter in operations on public roads and, within each scenario, the minimum set of assumptions that shall be considered to increase driving safety. As Figure 1 illustrates, the minimum set of reasonably foreseeable assumptions defined by this standard includes properties of other road users, such as velocity v, heading h, rate of change of the heading angle h', braking capabilities β, and response times ρ.

Next, the "Common Attributes of Suitable Safety-Related Models" section identifies a summary set of recommended attributes for safety-related models used in the dynamic driving task. To arrive at this list, the WG conducted a literature review of contributed safety-related models, including sources on responsibility-sensitive safety,[3] the Safety Force Field,[4] rule books,[5] and others. Finally, the "Verification Methods for Assumptions Used in Safety-Related Models" section identifies techniques, such as various design and testing processes, that can be used to verify whether the implementation of a safety-related model conforms to the minimum set of required reasonably foreseeable assumptions defined in the standard.

The third draft of the standard is currently going through a final round of updates before it is shared via liaison agreements with the Society of Automotive Engineers and ISO for the first set of external reviews. The WG is targeting the second quarter of 2021 to submit the standard for balloting with the Vehicular Technology/Intelligent Transportation Systems Standards Committee and to simultaneously initiate a 60-day public review period. The goal is for this standard to be officially published by the end of 2021.

IEEE P2851

The IEEE P2851 goal is to provide an exchangeable and interoperable format



Ego Vehicle Is Turning Right at Intersection With Another Road User Blocking Visibility of Potential Incoming Traffic

Ego Vehicle Is Turning Left at Intersection With Another Road User Blocking Visibility of Potential Incoming Pedestrians at Crosswalk

Ego Vehicle Is Turning Right at Intersection With Limited Visibility Due to a Parked Vehicle

Ego Vehicle Is Turning Right at Intersection With Limited Visibility Due to Static and Dynamic Objects in the Scene

FIGURE 1. A scenario of an intersection with occlusions from IEEE P2846-D2.

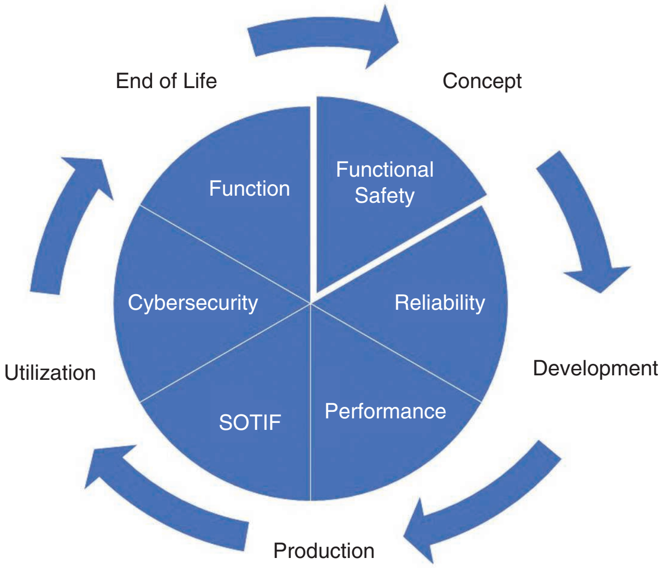


FIGURE 2. A representation of the IEEE P2851 PDL. SOTIF: safety of the intended functionality.

for safety analysis and verification activities to facilitate intellectual property (IP) and system-on-chip (SoC) providers to deliver results to safety-critical system integrators in a consistent way and also enable interoperability among tools provided by electronic design automation (EDA) tool vendors. IEEE P2851's initial scope was IPs and SoCs, but it has been extended to include items, systems, and SW as well. Artificial intelligence is also a key part of the activity. The WG has representatives from 31 entities, including all of the major IP/SoC providers, EDA vendors, Tier 1s, and OEMs. It is led by NVIDIA (chair and secretary) and Qualcomm (cochair).

The development of IPs and SoCs for safety-critical applications is emerging rapidly because of the growth of

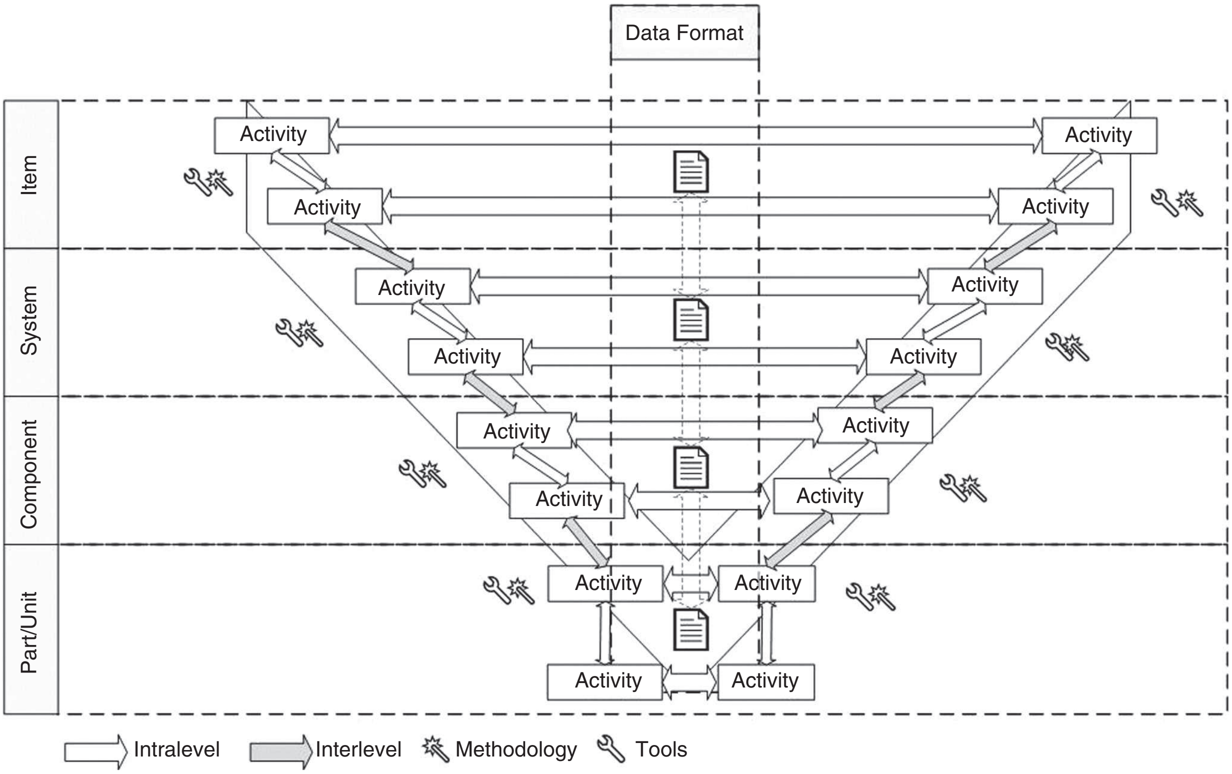


FIGURE 3. An IEEE P2851 landscape representation.

applications such as automated driving and robotics. Standards such as ISO 26262 (automotive),[6] IEC 61508 (industrial),[7] and many others require IP and SoC providers to execute safety analysis and related verification activities and deliver results to system integrators. EDA vendors are starting to provide tools to automate activities; however, at this time, there is no common language or format to provide the results. For that reason, the safety-critical community is demanding a solution to accelerate the safety engineering process while reducing risks and costs.

IEEE P2851 will define a data format with which results of safety analyses and related safety verification activities 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 results of the analyses and verifications can be represented in a technologically independent way. IEEE P2851 will provide a common ground for EDA, SoC, and IP vendors to develop tools, SoCs, and IPs for safety-critical applications.

The end goal is for IEEE P2851 to become a family of standards (P2851.1, P2851.2, P2851.3, and so on) covering broader functional safety topics, such as system- and SW-level safety analyses and formal/semiformal representations of assumption of use, and also extending to adjacent domains, such as cybersecurity analyses and related verification methodologies.

IEEE P2851 defines a dependability landscape based on an overall product dependability lifecycle (PDL), as represented in Figure 2. The word *dependability* has been selected to cover the broad spectrum of functional safety, safety of the intended functionality (SOTIF),[8] cybersecurity, and other characteristics, such as reliability, maintainability, and real time.

The landscape is represented based on a V-model, as shown in Figure 3. Each level (item, system, component, and part/unit) includes one or more activities belonging to phases of the PDL. Activities are connected with intra- or interlevel interfaces. Each activity can be linked to methodologies and tools to be executed.

Currently, the IEEE P2851 WG members are working on the landscape use-case activities within six subgroups: Automotive Functional Safety, Artificial Intelligence, Avionics, Security, Industrial/Medical/Robotics, and SOTIF. By the end of March 2021, the WG is scheduled to publish a white paper based on the first version of the landscape document, describing the lifecycle activities and related needs of methodologies and tools. By 2021 year's end, the plan is to release a first draft of the standard, and by the end of 2022, a final version of the standard will be published. C

REFERENCES

1. "Assumptions for models in safety-related automated vehicle

behavior," IEEE Standards Association, Piscataway, NJ. Accessed Feb. 2021. [Online]. Available: https://sagroups.ieee.org/2846/

2. "Exchange/interoperability format for safety analysis and safety verification of IP, SoC and mixed signal ICs," IEEE Standards Association, Piscataway, NJ. Accessed Feb. 2021. [Online]. Available: https://sagroups.ieee.org/2851/

3. S. Shalev-Shwartz, S. Shammah, and A. Shashua, "On a formal model of safe and scalable self-driving cars," 2017. [Online]. Available: https://arxiv.org/abs/1708.06374

4. D. Nistér, H.-L. Lee, J. Ng, and Y. Wang. "The safety force field." NVIDIA.com. https://www.nvidia.com/content/dam/en-zz/Solutions/self-driving-cars/safety-force-field/the-safety-force-field.pdf (accessed Feb. 2021).

5. A. Censi et al., "Liability ethics, and culture-aware behavior specification using rulebooks," 2019. [Online]. Available: https://arxiv.org/abs/1902.09355

6. *Road Vehicles—Functional Safety*, ISO 26262, 2018.

7. *Functional Safety of Electrical/electronic/Programmable Electronic Safety-Related Systems*, IEC 61508, 2010.

8. *Road Vehicles—Safety of the Intended Functionality*, ISO/PAS 21448, 2019.

RICCARDO MARIANI is the vice president of industry safety at NVIDIA, Santa Clara, California, 95051, USA. He is the 2021 IEEE Computer Society first vice president and chair of IEEE P2851. Contact him at rmariani@nvidia.com.

NIR MAOR is a senior director of technology at Qualcomm Technologies, San Diego, California, 92121, USA. He is the IEEE P2851 vice chair. Contact him at nmaor@qti.qualcomm.com.

JYOTIKA ATHAVALE is a senior functional safety architect at NVIDIA, Santa Clara, California, 95051, USA. She also serves on the IEEE Computer Society (CS) Board of Governors and the core team of the CS Special Technical Community on Reliable, Safe, Secure and Time-Deterministic Intelligent Systems. Contact her at jathavale@nvidia.com.

KEVIN GAY is a senior program manager at Aurora, Pittsburgh, Pennsylvania, 15201, USA. He is the IEEE P2846 secretary. Contact him at kgay@aurora.tech.

Digital Object Identifier 10.1109/MC.2021.3059060