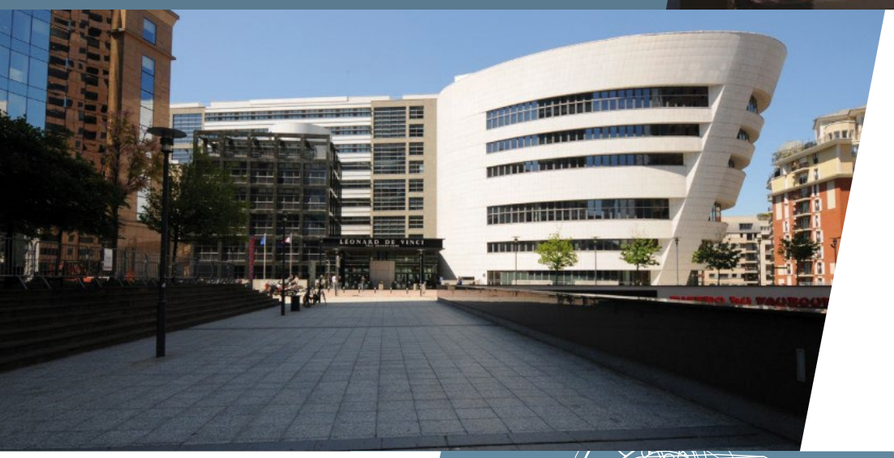
100 experts présents

JOURNÉE D'ÉTUDE **SIA ISO 26262**

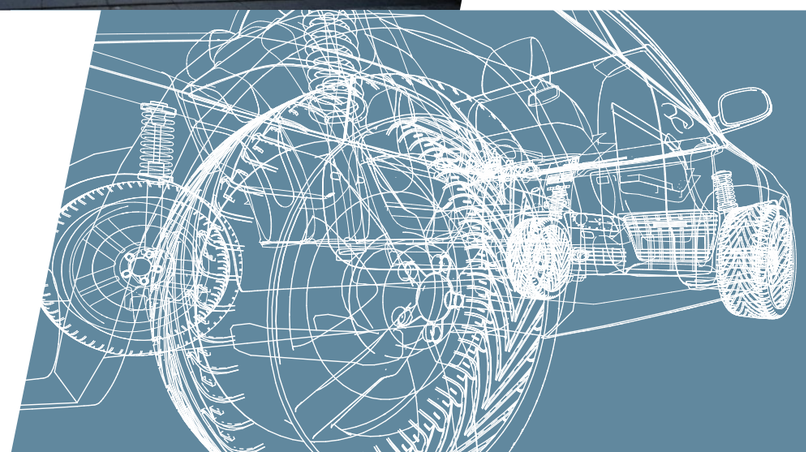
PÔLE LÉONARD DE VINCI
LA DÉFENSE
4 AVRIL 2018

Bruno Majot



3ème édition

5 exposants



La 3ème Journée d'étude SIA Norme ISO 26262 s'est tenue le 4 avril dernier au Pôle Léonard de Vinci à la Défense.

Plus d'une centaine d'experts s'est déplacés malgré les grèves des transports pour partager retour d'expérience et mise à jour des standards, tant sur les aspects organisationnels que techniques, des normes de la sécurité fonctionnelle électronique automobile à l'heure de l'accélération de la mobilité du futur à travers les véhicules autonomes et connectés.

Bruno Majot, leader du comité d'organisation de cette Journée d'étude SIA, a répondu à nos questions sur les thèmes et enjeux de ces rencontres. De plus, un papier de Nicolas Becker du Groupe PSA revient sur le SOTIF.

Pourquoi une 3ème édition consacrée aux normes ISO 26262 en 2018 ? Peut-on dire que les normes bougent beaucoup à l'heure de l'accélération des technologies automobiles ?

Bruno Majot : Avant tout parce que c'est notre rituel !!!
En fait lors de notre première journée fin 2013, Nicolas Becker avait conclu la journée par un constat qui allait bien au-delà de cette première journée de travail : il a souligné la naissance de la communauté d'expert ISO 26262.
Nous avions tous exprimé alors le besoin de se retrouver régulièrement pour :

- nous conforter quant aux actions mises en place dans chacune des entreprises,
- échanger sur des problèmes à résoudre,
- se sentir moins seul et plus fort au sein de notre communauté.

Il est donc important de nous réunir régulièrement pour systématiquement faire un retour vers le passé pour évoquer des avancées significatives et présenter les évolutions, notamment le « fameux » SOTIF.
Dernier point important en 2018 qui concerne l'ISO 26262, c'est l'élargissement de son périmètre avec la prise en compte désormais des poids lourds, bus et 2 roues motorisés.

Le monde automobile s'est transformé depuis deux ans et la dernière Journée d'études ISO, quels sont les principaux changements et enjeux nouveaux pour tous les experts présents ?

Bruno Majot : Cedric Heller, de PSA nous a dressé un tableau des principales évolutions du cru 2018 :

- Nouveaux périmètres : Poids Lourds et Bus (évoqués tout au long des « parts actuelles »), 2 roues motorisés (faisant l'objet d'une nouvelle « part 12 »)
- Nouveaux sujets : concept Fail Operational, une nouvelle part 11 pour les semi-conducteurs
- Des restructurations profondes, notamment sur les « Confirmations Reviews », sur l'« initiation of product development » et sur le traitement des anomalies Safety
- Des précisions sur différents thèmes
- Un lien avec les activités « Cybersécurité »
- Un lien avec le traitement du « fonctionnel sûr », le fameux SOTIF à travers le PAS 21448

L'après-midi était consacré au véhicule autonome notamment, que retenir à court et moyen terme sur le lien entre l'émergence des techniques du VA et les normes Iso de sécurité dont on sait que c'est l'enjeu majeur du développement de la mobilité autonome ?

Bruno Majot : L'ISO 26262 a pris en compte l'émergence des techniques du VA principalement sur 3 aspects :

- La prise en compte du concept Fail Operational qui consiste à concevoir des architectures E/E capables d'être tolérantes à la première panne pour pouvoir, a minima, mettre le véhicule en sécurité après l'apparition d'une panne.
- La prolongation de la maitrise du dysfonctionnel par la prise en compte du « Fonctionnel Sûr » (SOTIF : Safety Of The Intended Functionality). En effet, si on prend par exemple les fonctions de perception du VA, comment démontrer, qu'en absence de panne, les performances des capteurs sont au rendez-vous et sont suffisantes pour participer aux actions de pilotage du VA en toute sécurité ?
- Quel est le niveau de performances intrinsèques de ces technologies du VA puisque l'idée est de remplacer la vision et les actions du conducteur par des technologies ?

Le monde des Normes ISO et sécurité est donc aussi en pleine mutation et quels sont pour vous ses principales perspectives, inquiétudes et enjeux ?

Bruno Majot : L'arrivée de l'ISO 26262 il y a 7 ans maintenant n'a pas vraiment « révolutionné » le monde automobile mais a permis de définir un standard atteignable par la profession. Les bonnes pratiques se sont propagées par divers moyens (accompagnements de constructeurs vers leurs fournisseurs, fournisseurs de rang 1 moteur dans le déploiement du standard, formations… dispensées par la SIA,…).
Mais tout ceci a pris du temps, des ressources, de l'énergie.
Quand on aborde les aspects « Sûreté de Fonctionnement », il y a d'autres performances à adresser : la fiabilité, la disponibilité, la maintenabilité, la durabilité,…) et ce aussi bien sur les aspects E/E que sur les autres technologies (la mécanique entre autres) et bien sûr en abordant les risques produits mais aussi les risques process.
Ma principale inquiétude est d'avoir finalement un volume de ressources suffisant pour traiter la safety E/E et qu'en revanche les autres performances de la SdF, les autres technologies, les aspects process fassent un peu les frais de ce standard.
Une discussion récente avec un responsable de la sécurité du produit d'un constructeur m'a conforté en effet dans le fait que les principaux « ennuis » actuels ne sont pas sur la conception des ADAS mais bien sur des problèmes plus « classiques » (mécanique, process,..)
Ma conclusion est donc de ne pas mettre tous ses œufs dans le même panier mais de traiter aussi les « anciennes technologies » en safety, de consacrer de l'énergie sur les aspects process et de faire des voitures qui roulent !!!

Article de Nicolas Becker

The Safety of the Intended Functionality : Failures are not the only system safety problem…

Nicolas Becker graduated in 1994 from the Ecole Nationale Supérieure de l'Aéronautique et de l'Espace (ENSAE/SupAéro). He joined PSA in 1995 and held several positions in the development of safety-related systems and components. He was appointed Functional Safety Senior Expert in 2007. He is the convenor of the French WG8 mirror group, and of the SOTIF Task Force at the ISO/TC22/SC32/WG8.

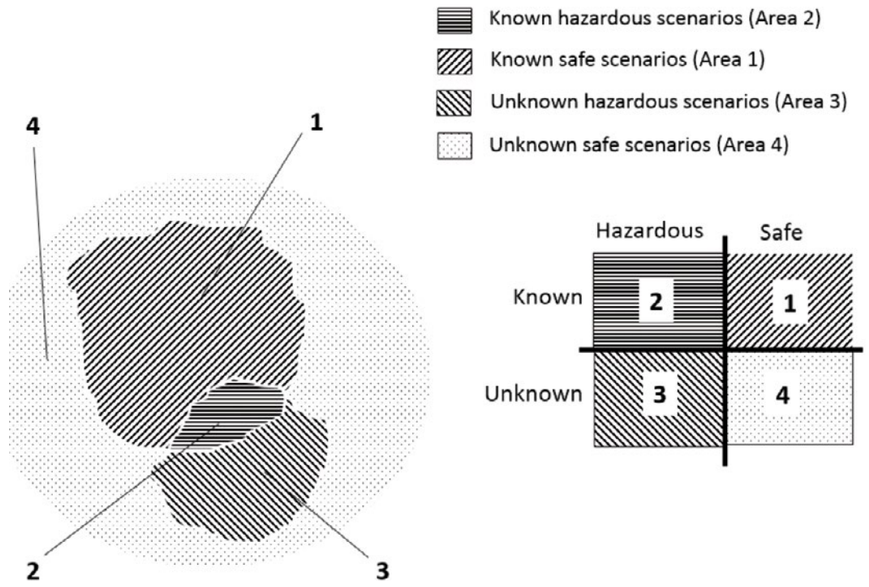
Recent years have shown an increasing adoption of Advanced Driving Assistance Systems (ADAS), including Adaptive Cruise Control (ACC), Lane Keeping Assist (LKA), Automated Emergency Braking (AEB), etc. These systems typically include sensors to perceive the environment, a decision making algorithm and issue commands to the vehicle actuators (steering system, braking system, engine…) to provide their function to the driver.
From a safety perspective, an incorrect or unwanted action by such systems may lead to safety-relevant consequences, depending on the actuation level and the life situation. The ISO 26262 series of standards, published in 2011, provides guidance to identify and address the risks caused by faults in the system : random hardware component faults, systematic failures such as software bugs, etc.

However, such advanced systems might lead to potentially hazardous system behavior in the absence of the faults addressed in ISO 26262, for instance:

- If the sensors classify the situation incorrectly and forward an incorrect environment representation to the decision algorithm;
- If the decision algorithm takes a decision inappropriate to the life situation,
- If the actuator performance limitation leads to an incorrect vehicle behavior

An example of such a system is a camera-based Automated Emergency Braking System, whose function would be to activate the host vehicle brakes upon detection of a slow-moving vehicle in front of the host vehicle to avoid a collision. If the camera mistakes a traffic sign for a target in front of the host vehicle, it could decide to activate the emergency braking, which could lead to rear –end crash with a close-tailing vehicle.
Another possible cause for hazardous behavior is the system-user interaction, including possible misuse of the system.
To provide guidance for these classes of risks, the ISO/TC22/SC32/WG8 – already responsible for the ISO 26262 standard – appointed a task group to develop a dedicated document. It was prepared between 2015 and 2018, and will be published this year as a Publicly Available Specification: the ISO PAS 21448. The scope of this PAS includes the ADAS functions of Level 1 and 2 (ADAS under the driver's supervision). It may be applied to higher levels of automation, but additional measures are likely necessary.
The PAS is based on the idea that a system will be faced with a wide variety of life situations in its operational life, and that the behavior it has in each of those situations must be free from an unreasonable level of risk. The intended 'nominal' functionality is improved and validated to achieve this objective as necessary. This defines the Safety of the Intended Functionality (SOTIF).
At the beginning of the SOTIF activities, an initial function and system description is described, and an hazard analysis is conducted to identify the hazards that an incorrect system behavior could trigger. This phase is similar to the 'Hazard Analysis and Risk Assessment' described in ISO 26262-3.
The scenarios faced by the system during its operational life are classified along two modalities:
-Known/unkown : has this scenario been identified and classified?
-Hazardous/Safe : is the system prone to a potentially hazardous behavior in this scenario?

The purpose of the SOTIF activities is to reduce the known hazardous scenarios by improving the system (Area 2), and to show through verification and validation that the residual risk due to potentially hazardous unknown scenarios is sufficiently low (Area 3).
To achieve this purpose, a systematic analysis of the driving scenarios is performed, considering the functional and system description and the hazard analysis, to identify the 'triggering events' that can cause a potentially hazardous



behavior of the system (the presence of the traffic sign in the AEBS example above). The user-system interaction analysis is also conducted in this first phase.
A first loop of system improvements is conducted until the analysis shows an acceptable level of coverage of the identified scenarios.
The SOTIF activities continue with the verification, to check if the system behavior is consistent and safe in the known identified scenarios. Any potentially hazardous finding leads to a further loop of functional improvement

Finally, the validation activities aim at confirming that the residual risk due to unknown scenarios is sufficiently low. For this, the argumentation is based on a combination of methods including long-term captured fleet test, randomized simulations, etc. Identified previously unknown hazardous scenario also lead to functional improvements.
Possible functional improvements include :

- Improvement of the sensor and/or algorithms performance
- Reduction in the actuation pattern to improve driver's controllability
- Restriction of the system activation to known safe scenarios (for instance, deactivation of a camera-based functionality if it is blinded by the setting sun).

The PAS provides guidance to justify the amount of required validation for the functionality.
It also includes guidance on the machine learning algorithms, who are increasingly used on this kind of systems.
The PAS21448 will be turned into a full ISO standard under the ISO21448 reference, under the supervision of the WG8 working group. Its publication is envisioned for 2022. Meanwhile, the PAS provides the industry and the other stakeholders with a guidance to support the safety demonstration for this class of systems, whose intrinsic design is already a key safety issue