Focus Day: Safety in Machine Learning

8.30 am Registration for Focus Day

9.00 am – 10.00 am | **State-of-the-art Machine Learning**
Machine Learning is the new buzzword when talk is about highly automated driving, notably with respect to safe functionality of highly automated and autonomous vehicles. Learn in this introduction presentation what the state-of-the art Machine Learning is, and what companies play a key role.
- Current status in Machine Learning, and its development
- Companies you should keep track of when it comes to Machine Learning
- Roadmap for the next 20 years – what you can expect

DENSO **Dr. Chih-Hong Cheng,** Technical Manager, **DENSO INTERNATIONAL EUROPE**

10.00 am Refreshment break and networking

10.30 am – 12.30 pm | **Towards validation of Machine Learning Systems**
Now that you are introduced into the current status in Machine Learningdevelopment, a discussion will follow on some of the most promisingmethods and present challenges in the verification of Machine LearningSystems. This will involve a hands-on session in which you discuss withpeer players in the market about how safety in Machine Learning could bedefined. This will include: Understand the potential pitfalls of using Machine Learning inautomated driving- Reflect on the present state-of-the-art on verification of Machine Learning systems, including strengths and present challenges- Contribute to the discussion on what are the key challenges that needto be solved in terms of specifications and verification before MachineLearning can be regarded as safe for deployment

Audi **Dr.-Ing. Vahid Hashemi,** R&D Project Manager, Dependable AI/ML Systems, **AUDI AG**

Imperial College London **Prof. Alessio Lomuscio,** Professor of Computer Science, **Imperial College London**

12.30 pm Network Luncheon

1.30 pm – 2.30 pm | **Machine Learning, Full Autonomy, and Safety Standards**
ISO/PAS 21448 safety of the intended function (SOTIF) has an important role to play in ensuring highly automated driving. However, once a human is not constantly supervising the system, additional challenges arise that can be further addressed by combining SOTIF concepts with UL 4600.
- Roles of ISO 26262, ISO/PAS 21448 SOTIF and UL 4600 safety standards in assuring autonomous vehicle safety
- Validating perception and dealing with perception brittleness
- Going beyond just the dynamic driving task for safety of fully autonomous vehicles.

EDGE CASE RESEARCH **Philip Koopman**, CTO, **Edge Case Research**

2.30 pm – 4.30 pm | **Hands-on workshop: How to apply and test for safety criteria in Machine Learning for highly automated driving**
While no-one is able to predict the AI learning process, safety needs to be assured to an acceptable level. Get insights into an approach for safe Machine Learning, and elaborate in this hands-on workshop yourself the best way to apply and test for safety criteria in Machine Learning for you and your business.
- Exchange with key market players on their experience and lessons learnt
- Define test criteria for safe Machine Learning
- Identify the best way for you and your business to achieve safe Machine Learning

VOLVO *The focus day is moderated by:*
Carol Farber, Product Safety Leader Electromobility GPE Wheel Loaders, **Volvo CE**

KICKING OFF THE MAIN CONFERENCE | MONDAY, 30 SEPTEMBER 2019

4.30 pm Registration for main conference and coffee

5.00 pm **Safety for highly automated driving**
Let's kick off our conferences by looking into the industry's understanding on safety concepts for highly automated and autonomous driving.
VOLVO **Carol Farber,** Product Safety Leader Electromobility GPE Wheel Loaders, **Volvo CE**

5.30 pm **Ice-breaking Round Tables**
Get to know the other participants by discussing future mobility!
A. Will robot cars dominate our future?
B. Flying cars
C. Your dream car

6.15 pm **Informal Evening Get-Together** | Join our evening Get-Together and take this opportunity to network and make new business contacts. Or just to relax and round off your first conference day.

CONFERENCE DAY 1 | TUESDAY, 1 OCTOBER 2019

8:00 am Registration and welcome coffee

Who is Who | Discover who else is participating in the conference. The matchmaking picture wall will help you identify who you want to meet at the conference. In cooperation with FUJIFILM

9.00 am Opening remarks by the conference chairman
Kyle Post, Systems Engineering and Functional Safety Technical Leader, **Ford Motor Company**

Keynote Opening Presentation

9.10 am **Scene Setting | Current status of ISO/PAS 21448 – Safety of the intended functionality (SOTIF)**
This introductory presentation aims at wrapping up the main achievement in the first draft of SOTIF. It will further introduce topics that have been discussed in the last SOTIF working group meeting.
- Overview on the composition of the standard
- Insights into the development process of ISO/PAS 21448:2019
- Roadmap to ISO 21448 withdrawal

Dean Degazio, Chief Engineer, Autonomous Driving Safety, **Aptiv**

9.50 am **Mix N' Match |** This is the time to get out of the comfort of your chair and get to know who else is in the conference room with you. A networking facilitating session designed just for you to help you break the ice as early as possible.

10.30 am Coffee break and networking

DEFINING SAFETY OF THE INTENDED FUNCTIONALITY

11.00 am **The scope of SOTIF, compared to the one of ISO 26262**
Originating from ISO 26262, the ISO/PAS 12448 SOTIF tackles hazardous behavior of a system that is free from E/E system faults. In this, SOTIF complements ISO 26262.
- Clarity of scope of SOTIF and ISO 26262
- System based hazards and hazards caused by external factors
- Real world examples underlining the need for SOTIF

Hakån Sivencrona, Safety Program Manager ADS, **Zenuity**

11.40 pm **Expert Panel Discussion | Intended functionality on vehicle level**
Originally evolving from ISO 26262, the standard of the intended functionality goes one step further than looking at functional safety on item level, but widens the view to the vehicle level. How can this work? Who is responsible for what part?
Moderator
Gareth Price, Functional Safety Manager, **McLaren Applied Technologies**
Panelists
Dean Degazio, Chief Engineer, Autonomous Driving Safety, **Aptiv**
Hakån Sivencrona, Safety Program Manager ADS, **Zenuity**
Ali Houry, Engineering Manager Functional Safety, Autonomous Driving Systems, **American HAVAL Motor Technology**

12.20 am **SOTIF – another dimension?**
- Bosch approach to SOTIF activities on both sides of the V-model
- Challenges of statistical arguments, call for a better framework
- Example application of SOTIF activites to a perception problem

Miklós Halász, Functional Safety Expert - ADAS, **Robert Bosch Llc.**

1.00 pm Network luncheon

HAZARDS & TRIGGERING EVENTS

2.30 pm **Grab the chance! Part 1 |** Take 10 minutes to think of the one question on ISO/PAS 21448 that causes you sleepless nights – write it down, and it will be answered by a SOTIF working group member tomorrow.

2.40 pm **How to identify and analyze hazards**
Vehicle safety demands the avoidance of unreasonable risk caused by hazard caused by the intended functionality.
- Overview on hazards SOTIF is addressing compared to ISO 26262
- How to identify hazards caused by the intended functionality
- Hazard analysis and risk evaluation

Nathan Gallaher, Staff Systems Engineer, **Toyota Research Institute**

3.20 pm **STPA: A systems approach to autonomous vehicle safety**
The SOTIF standard is available, but how will you implement it? This presentation will explain how STPA, referenced in the new standard, can be applied to complex systems like autonomous vehicles.
- Potential design flaws and inadequate requirements can be prevented and addressed earlier when they are least expensive to fix
- A comprehensive set of potential problems can be identified, including both failure and non-failure cases
- A case study of STPA applied to an autonomous vehicle will be presented.
- Software, human interactions, and public road testing will be examined

John Thomas, Executive Director, Safety and Security group, **Massachusetts Institute of Technology (MIT)**

4.00 pm Refreshment coffee and networking

PREDICT THE UNINTENDED FUNCTIONALITY

4.30 pm **On-Line uncertainty prediction and unintended functionality diagnosis in autonomous vehicles**
With the intention of producing efficient, reliable, predictable and safe artificial intelligence based advanced technologies applied into autonomous vehicles, techniques applied into aeronautics and nuclear industries may give us a guide that should apply to automotive industry as well. This presentation propose a technique to predict and diagnose the uncertainty of ADAS bias caused by unacceptable triggering events that could lead to a hazardous event with a probable driver harm.

- Analysis and identification of unknown triggering events
- STPA and Event Tree Analysis
- On-Line prediction and diagnosis of Unintended Functionality due to triggering events using ANNs
- ANN uncertainty prediction based on error estimation by series association (EESA)
- ANN effectiveness and performance testing

MAGNA **Miguel Marina**, Functional Safety Engineer, **Magna International**

5.10 pm **Methods and process for best utilization of SOTIF and ISO 26262 standards**
The main objectives of the presentation are: first, leverage the well-known methods and process to define a unified approach to conduct the foreseeable misuse scenarios which could lead to a degraded functionality, second, attaining reasonable coverage of the test cases and real time scenarios which used to prove the safety case additional to ensure that the residual risk is reduced to a sufficient and acceptable level.
veoneer **Kholoud Hatem**, Functional Safety Manager, **Veoneer**

5.50 pm Closing remarks by
Ford **Kyle Post**, Systems Engineering and Functional Safety Technical Leader, **Ford Motor Company**, and end of conference day 1

6:10 pm **Evening Get-Together** | Join our evening Get-Together and take this opportunity to network and make new business contacts. Or just to relax and round off your first conference day.

CONFERENCE DAY 2 | WEDNESDAY, 2 OCTOBER 2019

8.30 am Registration and welcome coffee

9.00 am Opening remarks by Kyle Post

ISO/PAS 21448 AND SEMICONDUCTORS

Keynote Opening Presentation

9.10 am **The impact of ISO/PAS 21448 SOTIF on the semiconductor industry**
Part 11, solely focusing on the semiconductor industry, was just recently added to the ISO 26262 standard. This speech focusses on the impact the ISO/PAS 21448 will have on the semi conductor industry, e.g. on sensors verification and validation. Riccardo Mariani, leader of ISO 26262 part 11, explains if SOTIF will also need or not a dedicated chapter or annex on semiconductors. In this case, Riccardo is represented by his colleague Frank Noha.
Frank Noha, Safety Specialist, **NVIDIA**

9.50 am **Leveraging deep neural networks to ensure autonomous vehicle safety**
This presentation will specifically delve into how the integration of Deep Neural Networks (DNNs) for autonomous driving is impacting traditional development approaches, and how OEMs, Tier1s, and Tier2s can work together to build safer AVs through DNNs.
- Role of DNNs in autonomous driving
- Traditional development approach
- OEM/Tier1/Tier2 collaboration challenges (Performance and safety optimization for complex hardware, DNN training, Adaptation of trained DNNs for new vehicles, DNN compliance with SOTIF, V&V of DNNs)
- Future challenges

Frank Noha, Safety Specialist, **NVIDIA**

10.30 am **Grab the chance! Part 2 |** Find your right group to get the answer to your most important question!

Hakån Sivencrona, Safety Program Manager ADS, **Zenuity**
Gareth Price, Functional Safety Manager, **McLaren Applied Technologies**
Kyle Post, Systems Engineering and Functional Safety Technical Leader, **Ford Motor Company**
Dean Degazio, Chief Engineer, Autonomous Driving Safety, **Aptiv**

11.10 am Coffee break and networking

SAFETY ARGUING VALIDATION AND VERIFICATION

11.40 am **Safety arguing for (highly) automated driving systems**
The higher a system climbs up the automation level, the more complex it becomes to prove its safe functionality. This presentation gives an overview on safety analysis and safety argumentation foreseen by SOTIF.
- Safety Analysis recommended by SOTIF
- Safety argumentation according to SOTIF
- Best Practice example

Ali Houry, Engineering Manager Functional Safety, Autonomous Driving Systems, **American HAVAL Motor Technology**

12.20 pm **Statistical valdiation of ADAS functions**
With the extremely high amount of possible driving scenarios, a statistical validation approach might be useful to show the functional safety of the vehicle.
- Overview of the statistical validation approach
- Integration into existing testing processes
- Enabling virtual validation

Oleg Kirovskii, Principal Engineer - Safety Analysis, **ZF Group**

1.00 pm **Coverage Driven Verification as an enabler for SOTIF**
Coverage Driven Verification is enabling SOTIF, by providing ways to explore hazardous areas, analyze and reduce risk, and achieve quantifiable safety metrics.
- In order to ensure AV & ADAS safety, a methodological approach for achieving sufficient driving scenarios coverage and providing safety metrics is required.
- SOTIF is acknowledging that, by breaking down the scenario space into 4 areas, and providing a process to systematically go over the unknown hazardous and known hazardous areas in order to provide an argument that they are sufficiently small and the resulting risk is acceptable.
- The Coverage Driven Verification methodology is enabling SOTIF, by providing means for exploration of the unknown scenario space, means for mapping hazardous scenarios into none-hazardous scenarios, and an ability for estimation & reduction of residual risk, using various techniques.

Gil Amid, Chief Regulatory Affairs Officer, VP Operations, Co-Founder, **Foretellix**

1.40 pm Luncheon and networking

3.00 pm **Round Table Session | Opening the floor for comments on the SOTIF draft**
The SOTIF draft was published and is open for commenting. Take the chance and discuss the guidelines with working group members.
Moderators:
Oleg Kirovskii, Principal Engineer - Safety Analysis, **ZF Group**
Gareth Price, Functional Safety Manager, **McLaren Applied Technologies**
John Thomas, Executive Director, Safety and Security group, **Massachusetts Institute of Technology (MIT)**

3.40 pm **How ISO 26262 & SOTIF influence the functional safety architecture, used technology and validation?**
- ADS - Safety of the Item in case of Malfunction (SOTIM), SOTIF and Safety-in-use: Fail-safe, fail-operational and resilience
- Effect on the Embedded Architectural Design: hardware, semiconductor and software
- Technology (i.e. Sensor, Algorithm) requirements and challenges, verification and validation

Hermann Kränzle, Functional Safety Expert, **TÜV Nord Systems GmbH & Co. KG**

4.20 pm Refreshment Break

SAFETY & SECURITY WITH AUTOMATED DRIVING

4.50 pm **What are the right safety target values for autonomous urban driving?**

Our mission at AID is to create autonomous driving systems (ADS) for the people. With every human driven vehicle that we replace by ADS, we want to reduce the risk for harmful accidents. Today, 90% of accidents are caused by human distraction or disobeying traffic rules*. ADS should outperform the human easily for these causes of accidents. We believe that our ADS should still be better than the human driver for the remaining 10% of accident causes.

But ADS will also introduce new causes for accidents by technical failures and systematic design errors of hardware and software, and insufficient safety performance including limitations of algorithms and sensors in unknown and unexpected situations. The appropriate level, to which the risk must be reduced, has major impact on the development and on the acceptance of the product by the society. Some well-established approaches exist in classical automotive industry for manually driven vehicles as well as in other industries like aviation, railways, machinery, chemical processing industry, nuclear energy production. We match these approaches with the specific challenges of ADS. For our target values, we take a deep look into the situations of our targeted Operational Driving Domains, such as Munich urban driving.

Bert Böddeker, Principal Engineer, Product Safety, **Autonomous Intelligent Driving GmbH**

5.30 pm **Safety interaction with Cyber-Security domain**

Technology progress creates new opportunities in automotive industry. The vehicles are more and more automated leading to the development of complex systems. For the time being to ensure the safety of these complex systems not only the functional safety but the Safety In Use and Safety Of The Intended Functionality must be applied too.

For creation of an AD concept the interaction between Safety and Cyber-Security is necessary. The topics of bridging Safety and Cyber-Security based on SOTIF perspective that will be discussed:

- Performance limitations of the system due to Cyber-Security threats
- Interactions between safety and security mechanisms
- Environment / infrastructure influence on vehicle system due to Cyber-Security threats
- Safety and Cyber-Security common goals

Catalin-Stefan Ionescu, System Safety Engineer, **Continental Automotive**

6.10 pm Closing remarks by Kyle Post and end of the main conference. See you in 2020!

WORKSHOP DAY | THURSDAY, 3 OCTOBER 2019

8:00 am Registration for workshop A and welcome coffee

A

8:30 am - 11:00 am

INTRODUCING SOTIF: HANDS-ON SESSION ON HOW TO INTERPRET ISO/PAS 21448

Even though the SOTIF working group is discussing the standard for years already, ISO/PAS 21448 is brand new to the market. Said to become binding for highly automated and autonomous vehicles, governments and car makers have their eyes turned to SOTIF. Time to get a good understanding on what the scope of SOTIF is!

- Distingish the scope of SOTIF from the one of ISO 26262
- Get involved into a typical validation process according to SOTIF
- Take the opportunity to clear all your question marks

Dean Degazio, Chief Engineer, Autonomous Driving Safety, **Aptiv**

11.00 am Network luncheon and registration for workshop C

C

12:00 am - 2:30 pm

SOTIF - WHAT IT MEANS FOR SEMICONDUCTOR COMPANIES

Safety of the indented functionality will impact not only the car makers and tier 1 supplier but will make its way all down the value chain to the semiconductor companies. In this workshop you will learn and discuss on what the ISO 21448 PAS means for the semiconductors, and how to integrate the standard into the company.

- Understand early on what semiconductor companies have to prepare for
- Get a clear picture on how semiconductor companies, tier 1 suppliers and car makers need to cooperate to make a vehicle SOTIF compliant
- Learn from other market players their approach to move forward with ISO/PAS 21448

Kenneth Freeman, Principal Functional Safety Consultant (Formerly Hella), Systems and Functional Safety LLC

2.30 pm Refreshment break and registration for workshop E

E

3:00 pm - 5:30 pm

HOW TO PERFORM STPA

The system theoretic process analysis (STPA) is a much discussed risk and hazard analysis method. As a top-down analysis, STPA emphasizes the system's dynamic behavior including automation interactions and human behavior. Join this workshop to get a hands-on approach how to perform STPA and it's relationship to the safety of the intended functionality.

- Get a summary of the most important aspects of the STPA
- Understand the difference between traditional techniques and STPA, and latter's advantages
- Perform an exemplary STPA and raise questions during the analysis process

John Thomas, Executive Director, Safety and Security group, **Massachusetts Institute of Technology (MIT)**

5:30 pm End of Workshop Day