9th International CTI Conference
30 March – 1 April 2020, Rochester, MI, USA

BEYOND ISO26262

SOTIF
Cybersecurity
Functional Safety

CHAIRMEN:

CARSTEN GEBAUER
Robert Bosch GmbH

DR DAVID WARD
Mira Ltd.

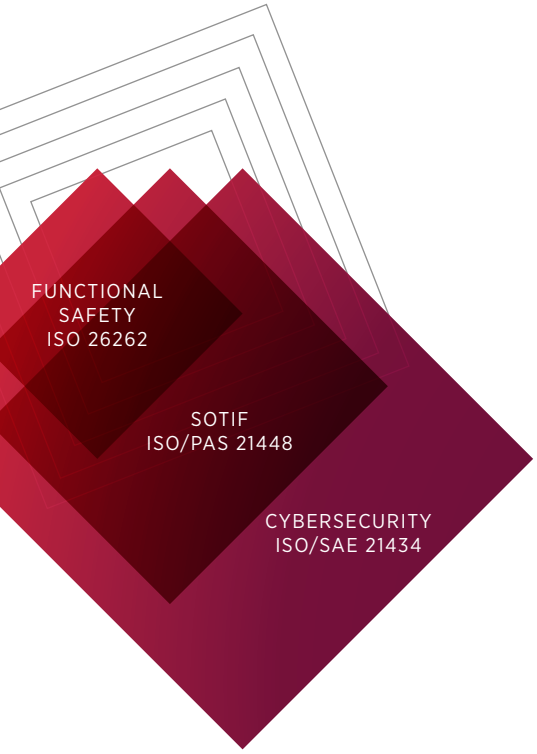
CTi

www.cti-iso.com

INSIGHTS FROM:
Bosch | DURA | FEV | Ford
General Motors | NVIDIA | MIRA
Schaeffler | and many more

9th INTERNATIONAL CTI CONFERENCE BEYOND ISO 26262

Functional Safety & SOTIF & Cybersecurity – Moving towards autonomous driving



Automated vehicles must be safe. A new standard is on its way – ISO/PAS 21448 – Safety Of The Intended Functionality (SOTIF). SOTIF is an important new concept that has been introduced alongside ISO 26262, to deal with wider aspects of system safety in the particular contexts of driver assist and higher levels of automated driving functions. ISO/PAS 21448 complements ISO 26262.

ISO 26262 also considers the need for functional safety interact with cybersecurity. ISO/SAE 21434 is under development in draft form but as it becomes established practitioners will need to consider areas of overlap and interaction more closely.

→ One conference – 3 interconnected topics

→ Benefit from best practices of 30+ experts

→ Valuable insights into most recent updates from working group members

CHAIRMEN

CARSTEN GEBAUER
Senior Expert, Bosch Center of Competence „Functional Safety“, Robert Bosch GmbH

DR DAVID WARD
Head of Functional Safety, MIRA Ltd.

ADVISORY BOARD

PROF. DR MANFRED BROY
Technical University of Munich

DR BARBARA CZERNY
DURA Automotive Systems

CARSTEN GEBAUER
Robert Bosch GmbH

KYLE POST
Ford Motor Company

PADMA SUNDARAM
General Motors Company

DR DAVID WARD
MIRA Limited

ARTAGUN YESILDERE
Robert Bosch LLC

MONDAY, 30 MARCH 2020

SOTIF & AUTONOMOUS DRIVING & FUNCTIONAL SAFETY

8.20 Reception and welcome coffee

8.50

Welcome address by the moderator

Carsten Gebauer, Senior Expert, Bosch Center of Competence „Functional Safety", Robert Bosch GmbH

9.00

ISO/PAS 21448: SOTIF – update and insights from the ISO working group

- Summary of the Luxemburg meeting
- New topics
- Outlook and timeline

Alexander Mirmilstein,
Customer Safety Engineer, NVIDIA

9.30 Q&A and discussion

9.40

The SOTIF mindset

Carsten Gebauer, Senior Expert, Bosch Center of Competence „Functional Safety", Robert Bosch GmbH

10.10

OMG Safety and Reliability

- Overview of the new object Management Group Model Based Systems Engineering (MBSE) standard for safety and reliability
- The new standard defines a standard graphical language for use to support ISO 21448 and ISO 26262
- Analysis methods included in the standard include HAZOP, ISO 26262 HARA, FTA, FMEA, STPA, and GSN

Kyle Post, Vehicle Systems Safety Supervisor, Ford Motor Company

10.40 Q&A and discussion

10.50 Coffee break

11.20

SOTIF risk management for different levels of automation

- Risk management
- Automated driving system
- SOTIF process


Hsing-Hua Fan, System Safety Engineer, General Motors
Krzysztof Pennar, System Safety Engineer, General Motors

11.50

Analytic based safety requirements development – supports SOTIF

- Process identifies gaps in the developed safety requirements and analysis
- Leverages analysis required of the standard(s) in the development and verification for completeness of resultant safety requirements
- Leverages safety requirements developed to verify completeness of safety analysis performed

Bhargav Chava,
Functional Safety Engineer, FEV

12.20

Comparison between FUSA and SOTIF from the perspective of a safety architecture

- Overview of safety architecture in the context of ISO 26262
- FUSA/SOTIF safety architecture comparison in SCDL application
- Status of SCDL standardization in ASAM
- Evolution of SCDL for autonomous driving system


Shuhei Yamashita, Principal Technical Expert/Senior Director, DNV GL Business Assurance Japan K.K.
Stephen Norton, Managing Director, Quint Safety GmbH

12.50 Lunch

1.50

Safety assurance case development for autonomous vehicles at General Motors

- Outlining safety assessment areas for autonomous vehicle development
- Creating a complete and consistent safety case across all safety assessment areas
- Utilizing Goal Structuring Notation (GSN) for safety case development


David Byars, Autonomous Vehicle System Safety Engineer, General Motors

Alison Bayzat, Autonomous Vehicle System Safety Engineer, General Motors

2.20

Manageable Safety Goals in ADAS

Dr Barbara Czerny, Technical Fellow Engineering, Functional Safety and Cybersecurity, DURA Automotive Systems

2.50

ASIL determination for fully autonomous vehicle functionality

- Inherent complexity of decision-making in ASIL determination for fully autonomous vehicle functionality
- Lack of differentiation between hazards in risk assessment for fully autonomous vehicle functionality
- Objective criteria for evaluating the complexity of autonomous vehicle functionality that mimics or replaces human decision-making

Dr Jeffrey Joyce, Managing Director, Critical Systems Labs, Inc.

3.20

MPS high ASIL power solutions – centralized vs decomposed

- Summarizing high ASIL architecture for power solutions
- Centralized solution pros, cons, and ADAS SoC example
- Decomposed solution pros, cons, and ADAS SoC example
- Deciding between centralized and decomposed safety architecture

Jing Y. Guo, Technical Marketing Functional Safety Manager, Automotive Monolithic Power Systems

3.50 Coffee break

4.20

Standardization of autonomous driving test scenarios – certification/licensing of autonomous vehicles

- Current initiatives for certifying autonomous vehicles across geographies
- Challenges/gaps in existing approaches
- Proposed stages for certification
- Recommendations on standardization of test scenarios & certification


Annie Paul, Competency Manager, TataElxsi

Nijesh Sadanandan, Senior Architect, TataElxsi

4.50

Model based safety goal development/verification (supports SOTIF)

- Safety goal development based upon application specific vehicle dynamic models
- Safety goal metric quantification to support required Pass/Fail criteria of both controls and validation
- Safety goal optimization, allowing the presence of a fault for as long a period as possible while vehicle remains in a safe state

Dr David LaRue, Functional Safety Engineer, FEV

5.20

End-to-end challenges for risk management when developing mechatronic products

Matthias Maihöfer, Head of Functional Safety, Schaeffler Technologies AG & Co. KG

TUESDAY, 31 MARCH 2020

CYBERSECURITY AS IT RELATES TO FUNCTIONAL SAFETY

8.20 Reception and welcome coffee

8.50

Welcome address by the moderator

Dr David Ward, Head of Functional Safety, MIRA Ltd.

9.00

Update on interactions between safety and security

- Risk assessment and risk management
- Product development lifecycle
- Assessment and assurance activities

Dr David Ward, Head of Functional Safety, MIRA Ltd.

9.30 Q&A and discussion

9.40

The role of the programming language in safety-/security-critical systems

- Review of ISO 26262 requirements for programming languages and comparison to DO-178
- Addressing safety and security concerns of object-oriented language features
- Hidden complexities of C++
- Influence on tool qualification

Dr Daniel Kästner, CTO, AbsInt GmbH

10.10

Automotive system exploitation in the era of ISO 21434

- Describe current methods of car hacking, and
- 1 – How these would be thwarted/prevented by correct implementation of ISO 21434
- 2 – How these would be successful given incorrect implementation of 21434
- Goal: Demonstrate that 21434 can solve lots of problems if done right, but the success thereof is in the hands of the implementers

Dr Karol Niewiadomski, Project Manager Functional Safety and Cyber Security, SGS-TÜV Saar GmbH

10.40

Cybersecurity effects on functional safety

- Translate cybersecurity terms into ASIL terminology

Issak Davidovich, VP R&D, C2A Security

11.10 Q&A and discussion

11.20 Coffee break

AGILE IN AUTOMOTIVE

11.50

Agile systems engineering for safety and security

- Systems engineering for automotive E/E development
- Safety and security requirements and systems engineering methods
- Scaling agile development for critical systems
- Ford case study

Jason Learst,
Business Development Manager, Vector North America Inc.

12.20

Agile model-based software development in the context of ISO 26262

- Automotive standards on agility (ISO 26262 and ASPICE 3.x)
- Agile approaches to model-based software development – the core concepts of agile methods like Kanban or Scrum
- Continuous integration in the context of agile software development: Elements of continuous quality assurance

Dr Jan Grabowski, Product Application Manager, Model Engineering Solution GmbH

12.50 Q&A and discussion

1.00 Lunch

PRACTICE WITH ISO 26262

2.00

Challenges of ISO 26262 Compliance & scenario-based verification for ADAS

- ISO 26262 compliance in “traditional” automotive innovation
- ADAS development challenges: Validation of neural network-based driving applications
- Case study 1: Application Lifecycle Management (ALM) tooling for Automotive SPICE, ISO 26262 and SOTIF
- Case study 2: Simulator based scenario validation of ADAS with ALM support

Prof Peter Haller, Senior Pre-Sales, Intland Software

2.30

New Challenges in the Automotive Sector – Status of Standardization

- Three of the most pressing challenges at the brink of the next phase of mobility: Cybersecurity, Complex Sensor Systems, Artificial Intelligence
- New ISO standards under development
- Actual status of standardization?

Stefan Goi, Functional Safety Engineer, TÜV Rheinland Group

3.00 Coffee break

3.30

Functional safety for batteries to support autonomous driving functions

- Meeting the stringent safety requirements up to ASIL D
- Avoiding conflicts with other non-safety and safety requirements
- Safety requirements development methodology including AUTOSAR implementation

Marilyn Rouet, Senior System Safety Engineer, IAV Automotive Engineering, Inc.

4.00

Challenges and lessons learnt in achieving ISO 26262 compliance for pre-existing software from a non-automotive domain

- Challenges with design and architecture
- Challenges with tools and tool certification
- Challenges with process and safety culture

Gurunath Ramaswamy, Principal Manager, Qualcomm Inc

5.00

CTI NETWORKING NIGHT

The CTI networking night is an opportunity to mingle with the participants, speakers, exhibitors and sponsors. Make new
business contacts in a relaxed atmosphere, discuss the topics of the day with your colleagues and peers while enjoying delicious food and drinks.

WEDNESDAY, 1 APRIL 2020

8.30 Reception and welcome coffee

LEGAL ASPECTS

9.00

Functional safety – best practice of product development from a legal perspective in the US and the EU

- State of the art and technology as legal terms and how to adapt them
- Agreements between supplier and customer – to be precise or not to be precise
- Communication and documentation – curse or blessing

Jeffrey Greene, Lawyer, Shareholder, Greenberg Traurig LLP

Daniel Wuhrmann, Attorney at Law (Germany), reuschlaw legal consultants

9.30 Q&A and discussion

9.50

Functional safety requires due care

- State of the art - legal basis of development
- Reliability - cornerstone for functional safety
- Use of consumer components in automotive applications?
- Testing – passport to SOP

Andreas Reuter, former Syndikus Corporate Legal Services, Robert Bosch GmbH

10.20 Coffee break

Wednesday, 1 April 2020

DEEP DIVE WORKSHOP INTRODUCING SAFETY OF THE INTENDED FUNCTIONALITY (SOTIF)

Dr David Ward, Head of Functional Safety, MIRA Ltd.
Steve Crozier, Senior Manager, Functional Safety, HORIBA CA, USA

In this workshop we will introduce the concepts and principles of SOTIF, the publicly-available specification ISO/PAS 21448, and some interactive case studies describing the SOTIF approach based on our practical experiences of applying the SOTIF PAS and wider activities.

10.50

Session 1 – introducing SOTIF

- Functional safety, SOTIF and the wider system safety context
- Brief overview of ISO/PAS 21448 "Safety of the intended functionality"
- SOTIF "area" concept for managing complexity and unknowns of automated driving scenarios
- Introduction to SOTIF approach to different "areas" of scenarios

12.30 Lunch

1.30

Session 2 – case studies

- Functional and system specification in the context of SOTIF
- SOTIF hazard analysis and risk assessment
- SOTIF risk reduction – verification, validation and acceptance
- Outlook and future directions of SOTIF

3.00

End of conference and workshop

The following partners already signed up:

kVA by UL

SGS

SGS TÜV SAAR

Exhibitor

AbsInt

KUGLER MAAG CIE besser mit uns

TÜVRheinland® Genau. Richtig.

Media Partner

IN COMPLIANCE

BECOME A PARTNER.

We'll be pleased to advise you:

Jörg Wiedenhöft, Sales Manager
+49 211 88743-3215
joerg.wiedenhoeft@euroforum.com

Euroforum Deutschland GmbH, Postfach 11 12 34, 40512 Düsseldorf

Your personal registration code

Internet-PDF

DIALOGPOST
Ein Service der Deutschen Post
ALLEMAGNE Port payé

BEYOND ISO 26262

Register online:
www.cti-iso.com/tickets
registration@car-training-institute.com

PRICE	Early Bird Price **until 10.01.2020**	2nd Early Bird **until 28.02.2020**	Regular Price **from 29.02.2020**
Beyond ISO 26262 **2 Day Ticket**	**2,050 $***	**2,400 $***	**2,700 $***
Beyond ISO 26262 **3 Day Ticket**	**2,650 $***	**2,950 $***	**3,400 $***

Automobile manufacturers special offer: **1,000 $***

GROUP DISCOUNTS:

1st Delegate 100% (full price)
2nd Delegate 20%
3rd Delegate and more 30%

* excl. VAT per person
A substitute may attend in your place at no additional cost.
The fee covers full digital conference documentation.

YOUR BENEFITS

As participant of a CTI event you receive the Handelsblatt business access free of charge for 3 months. This offer ends automatically. Handelsblatt GmbH will send you an email with all relevant access information. For this purpose we will make your contact details available to Handelsblatt GmbH. You may object to this free-of-charge service at any time.

YOU CANNOT ATTEND?

The forum documents are available two weeks after the conference at the price of 400 €*.
(For more information: +49 211 88743-3845)

You can find our terms and conditions online at: **euroforum.de/agben**

[P2300531]

www.twitter.com/CTI_symposium www.facebook.com/CTISymposium www.euroforum.de/news

INFOLINE

+49 211 88743-3845

For further information please contact:

CUSTOMER SERVICE AND REGISTRATION

Volker Altenbeck
+49 211 88737-3845
registration@car-training-institute.com

CONCEPT AND CONTENT

Elke Schneider, Conference Director
elke.schneider@car-training-institute.com

SPONSORING AND EXHIBITION

Jörg Wiedenhöft, Sales Manager
+49 211 88743-3590
joerg.wiedenhoeft@euroforum.com

YOUR VENUE

Royal Park Hotel Rochester, 600 East University Drive, Rochester, MI, 48307, US, +1 248-652-2600

In the conference hotel, there is a limited allocation of rooms available at a reduced price. Please arrange the room reservation directly with the hotel quoting the reference "CTI event".

NEED TO UPDATE YOUR CONTACT DETAILS?

Please call us or send an e-mail: +49 211 88743-3333, info@euroforum.com. You have the right to object to the use of your data for the purpose of direct advertising at any time. In addition, you have the right to demand information from us regarding the data about you that we have stored as well as the right to demand correction of incorrect data and the right to demand deletion in the event of inadmissible storage of data. You can contact our Data Protection Officer at "Datenschutzbeauftragter c/o Euroforum Deutschland GmbH, Toulouser Allee 27, 40211 Düsseldorf". In addition, you have the right to file a complaint with the supervisory authority.