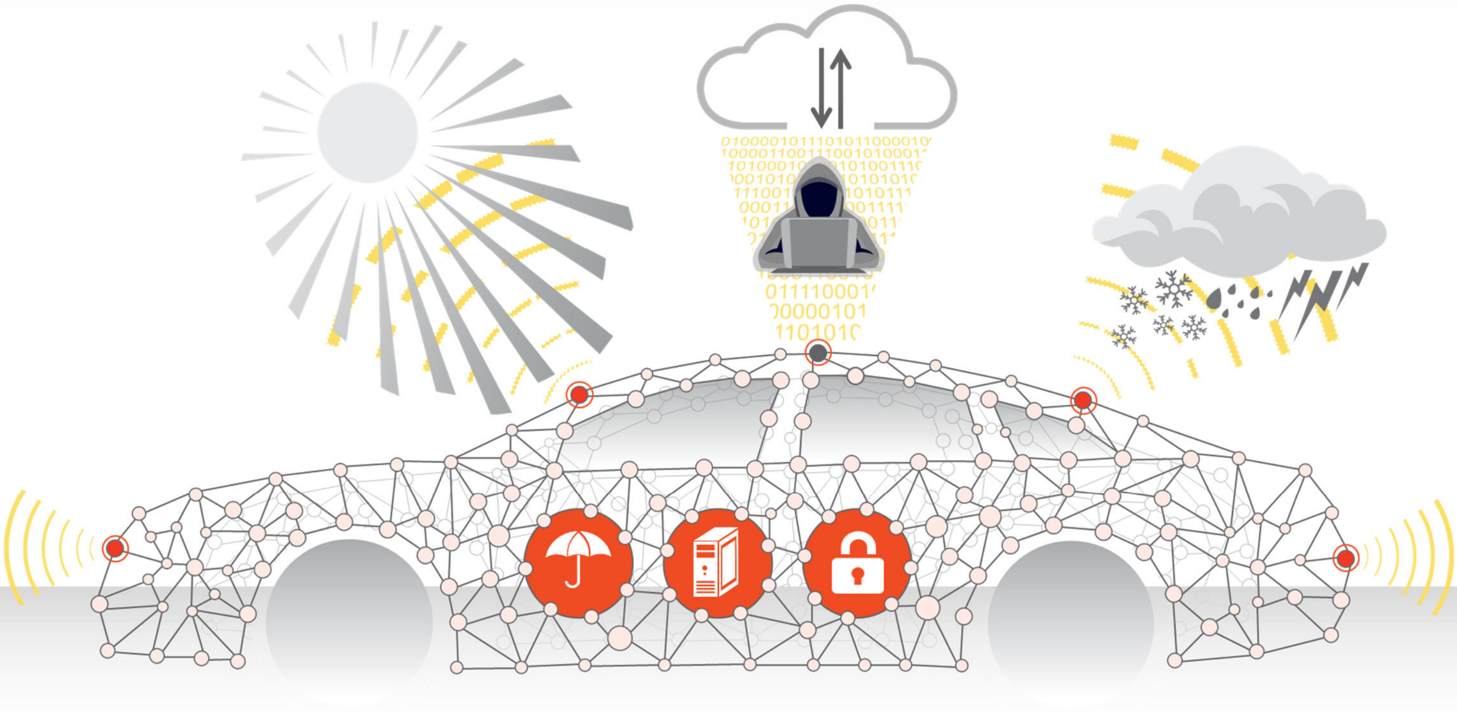
www.exida.eu



exida
Automotive Symposium 2022

Arabella Alpenhotel
am Spitzingsee

Seeweg 7
83727 Schliersee-Spitzingsee

exida.com GmbH
Zweigniederlassung
Prof.-Messerschmitt-Straße 1
85579 Neubiberg
www.exida.eu

exida Automotive Symposium 2022

Challenges in Functional Safety, Cybersecurity, SOTIF

On October 13 – 14, 2022 at Arabella Alpenhotel, Spitzingsee

SAE Level 5 driving automation remains an elusive but heavily research and invested goal of any organizations.

What is becoming clear are the increasingly higher performance and complexity computing solutions that are needed and currently being deployed.

New regulations from the European Commission are expected later this year. This will certainly increase the technical expectations placed on those developing, testing, releasing and approving highly automated vehicles that can drive everywhere and in all conditions.

exida is extremely pleased to invite expert contributions to our annual symposium representing key industry experts and thought leaders.

Key new safety concepts, technologies and approaches to safety and cybersecurity will be presented and discussed by the world-leading specialist.

We are looking forward to welcoming you to our 2022 Symposium.

For further information and registration please contact:

Kerstin Tietel
+49 89 44118232
kerstin.tietel@exida.com

Topics

Qualification of safety-related and complex Open-Source Software for high performance computing

The systematic and compliant re-use of pre-existing software for safety-related high performance computing is facing an ever increasing demand already in today's automotive projects. However, in reality success stories on these topics are rare due to the significant challenges which have been experienced and reported by safety experts along the automotive supply chain which often led to numerous project delays and the general belief that open-source reuse and safety are incompatible forever. In order to resolve these difficulties, standardization activities for “Qualification of pre-existing software for safety-related applications” have been started under ISO/AWI PAS 8926. Promising intermediate results are already available which will ensure that the automotive industry keeps its competitive edge also when reusing pre-existing software of unprecedented complexity and sizes and without sacrificing safety assurance rigor compared to the established approach for newly developed software. Current limitations in applicability of part 8.12 for qualification of complex pre-existing software have been investigated. Additionally required qualification activities from the existing standard have been systematically derived in the upcoming PAS 8926 and are expected to be integrated into future versions of part 8.12 - without breaking any backwards compatibility while at the same time extending safety compliance also for open source and complex pre-existing software. Short term economic savings by re-use in the sense of skipping safety activities unsubstantiated which might lead to compliance loopholes and severely less safety assurance rigor then compared to the part 6 approach are not to be expected. Likewise, “open-source safety paranoia” comes to its natural end as the new procedures will determine safety compliance rigorously on the same normative objectives and evidence like for newly developed software so the distinction is between suitable and unsuitable software for re-use on the same criteria. This can be exemplified on the importance of the development process - however not necessarily the original author's development process if the integrator's process can generate the required work products for the reused open source software, too.

Presented by Markus Schurius, BMW Group

ELISA (Enabling Linux in Safety Critical Applications)

With the increased complexity of HW platforms used in safety critical applications and increased complexity of safety critical workloads (e.g., autonomous driving applications) it is becoming more and more important to have a complex operating system that is able to support different HW platforms and different workloads and, at the same time, that is qualified to run safety critical application and to support mixed criticality (applications of different integrity level running in parallel).

Linux is functionally capable of accommodating all the demands above; now the main challenge is to qualify it for running safety critical applications. ELISA is a Linux Foundation projects that promotes the collaboration between different industry experts from different industry domains with the goal of producing useful material that can be freely re-used in different functional safety contexts to simplify and speed-up the Linux qualification process for safety critical applications.

This session provides an overview of ELISA, its missions, the goals and the current project structure.

Presented by Gabriele Paoloni, ELISA

Methodology for verification of transient fault metrics

Soft errors from single-event effects (SEE) are growing concerns in terrestrial automotive applications (in addition to data center, wired wireless applications, etc.) as devices are increasing in size and complexity. As single events (also referred as Transients) occurrence in programmable electronics, they can lead to systems failures in automotive systems and can manifest in physical injury of people or damage to properties. The automotive STD ISO-26262 ensures that the certified systems meet acceptable safety risk levels. Conventionally, fault injection is used for SEE error rate calculation and functional safety certification of programmable electronic systems which lead to high margin of errors & pessimistic results. In this presentation, accelerated particle beam test is performed as part of ISO-26262 certification for AMD AECG’s 7nm processors. We propose the beam test methodology to become a standard for ISO26262 certification.

Presented by Pierre Maillard, Paula Chen, AMD

Functional Safety in high performance SoC with heterogeneous architecture

AMD Versal SoCs offers a disruptive heterogeneous processing architecture for high performance compute systems in automotive, robotics and industrial applications. Achieving functional safety targets in such high-performance systems without consideration of system level solution is no go!

This talk provides insight into unique challenges and solutions to achieving functional safety in tiled architecture like the Versal AI Engine and Adaptable Engines.

Presented by Pramod Bhardwaj, AMD

Partitioning Functional Safety Requirements in an mmWave Radar Sensor System

This presentation discusses some of the key considerations and strategies to partition the functional safety requirements among the different components involved in the mmWave radar sensor system. The radar sensor system referenced in this presentation comprises of the TI AWR2944 Radar On Chip (RoC) device and TI LP8774x PMIC device. It also includes redundant communication paths via CAN and Ethernet that build the foundation for diverse signal processing in the sensor and central computer supporting aspects of the safety of the intended functionality (SOTIF). The partitioning of functional safety requirements is performed in a hierarchical manner. The AWR2944 RoC performs the safety monitoring functions of the Analog-RF operation, monitoring of the control and processing operations including corresponding safety diagnostic functions. The LP8774x PMIC device performs a system level monitoring of the RoC operation including program sequence monitoring, fatal error handling, voltage monitoring and ensuring the system is taken to a safe state in case of faults. The PMIC also shuts down the transceivers independently from the RoC when the sensor system enters into a fail silent state to isolate the external system from any spurious activity in case of faults.

Presented by Peter Aberl, Samir Camdzic, Sunil T V, Naveen Narayanan,
Texas Instruments

Achieving a Comprehensive Functional Safety Architecture From the Ground Up

Ambarella designs and builds high-performance, ultra-low-power SoCs capable of large-scale sensor fusion and simultaneous cutting edge AI acceleration—all designed in an automotive safety context. At the core of our SoCs is the CVflow® deep neural network (DNN) processing subsystem, now in its 3rd generation with the CV3 AI domain controller SoC family. CVflow has been purpose built to accelerate a wide range of AI workloads, and scales within the CV3 family to support L0-L5 automotive as well as robotics uses cases, spanning the edge to high performance central compute. By leveraging a functional safety process from the outset of our chip development, we establish a safety foundation from which all components of the SoC are built, while applying a keen focus on harmonizing system implementations in both the hardware and software domains. As demonstrated by the CV2FS family's ASIL C certification, our comprehensive approach achieves a high functional safety level for the entirety of the chip. In this session, we will discuss aspects of our methodology and provide insights from the design of our next-generation CVflow AI SoCs—the CV3 family.

Presented by Dr. Bob Kunz, Ambarella

Modelling and Arguing Fault Propagations in Complex Mixed-Criticality and Mixed-Compliance Software Systems

This presentation shows an approach on how to model a software architecture which enables the development of an argument on different aspects of freedom from interference in between architectural elements. The discovered concept is an application of viewpoints and views, a common tool in software systems architecture [1]. In our application, we use architectural elements of different safety compliance classes and refine the concept to tailor the scope of a view to a certain class of failure modes.

The approach is relevant to analyze software architectures in context of functional safety, containing elements of different origin and quality control. This situation is typical in open-source development, where some parts are developed by in-house development teams under a certain control of quality and other parts are developed jointly in the open-source community or by other third-party companies with little community engagement, leading to a different control of quality. The approach also allows us to analyze the interference between safety-relevant functionality and non-safety-relevant functionality. Throughout the presentation, we consider assessment of compliance to the IEC 61508 standard [2]. However, the concept is generic and can easily be applied to other functional safety standards, such as ISO 26262.

IEC 61508-3 allows the use of different compliance routes. Unfortunately, well-established viewpoints, such as those on functionality or architectural decomposition, lack the consideration and expression of compliance to a safety standard or a different route within a safety standard. We address this lack with our method: we define different safety compliance classes, for which each fulfils a compliance route as defined in IEC61508., and those compliance classes can then be characterized by attributes, such as the origin of software, its safety relevance, its exception level and optional further properties. The corresponding compliance arguments to those classes implicitly hold information on mitigation measures that ensure systematic capability of software. The systematic capabilities imply certain levels of freedom from interference and allow to construct an FFI argumentation. If that first level of detail is not sufficient for the FFI argumentation, finer-grained measures need to be referenced, which are deduced from the analysis on HW/SW interfaces or SW/SW interfaces.

Due to the multitude of aspects of FFI, we refine the presentation of the FFI argumentation: the arrows in between architectural elements need to express the type of fault propagation, e.g., following the classification according to IEC61508-3:2010 Annex F.3. The concept applied here is the one on equivalent circuits known from electrical engineering. The presentation explains the viewpoint developed and shows its exemplary use along examples on Linux.

Presented by Michael Armbruster, Lukas Bulwahn, Simon Friedmann, Julian Ott, Jens Petersohn, Elektrobit

Automotive: The forthcoming Statutory and Regulatory Perfect Storm

For many years, the automotive sector has enjoyed a special status among the transportation sectors; that of being largely self-regulated rather than being directly regulated by authorities. Key automotive standards such as ISO/TS 16949 (then IATF 16949), ASPICE, ISO 26262 and SAE J3061 (then ISO/SAE 21434) have always been taken up voluntarily and/or by market requests, never mandated by law.

Now, the tide seems to be reversing. We can identify the turning point in the publication of UNECE R155 and R156 on 4 March 2021; they establish that significant technical requirements for Cybersecurity and for SW Update Over-The-Air have to be certified before new vehicles can be ‘road-worthy’. Those regulations are not that thick (30 and 16 pages) but they are replete with technical specifications that have been usually left out of regulatory aspects in automotive.

Another new and big game changer is in preparation by the European Commission. A draft of Regulation 2019/2144 governing “modern technologies used in vehicles, including specific requirements for automated and fully automated (‘driverless’) vehicles and the systems they employ, to ensure that they are safe to use”, has been published on 07 April 2022, accompanied by 70 pages of technical Annexes, and it is expected to be finalized by mid-2022.

The actual impact of this ’tsunami’ of new regulations in a sector which is already struggling with overwhelming projects complexity is difficult to pinpoint, however, at least one thing is clear: roadmap to new standards/regulations compliance is no longer (just) in the hands of industry but (mostly) in those of the lawmakers: a paradigm shift.

Presented by Carlo Donzella, exida

Constructing complex systems from SEooCs

Complex safety systems in cars are increasingly composed of a multitude of interacting safety elements that have been designed out of context of the target systems by different suppliers. Research on autonomous driving platforms has shown that such a platform involves the integration of dozens of safety elements out of context (SEooCs) for both hardware and software. However, integrating these SEooCs is not straightforward.

This presentation identifies and discusses the issues and concerns involved in the safety integration task of SEooCs in complex safety systems.

Presented by Dr. Christopher Temple, ARM

How to ensure safety-related availability for L3-Systems on software level?

In modern vehicles safety-related availability is one of the key enablers for autonomous driving. Availability is a system property which ensures, that in case of a system failure or the driver's unresponsiveness, the system will continue to operate until the safe state is reached. This talk elaborates some important safety related availability aspects, which have to be considered on software level and formulates questions to support further investigation.

Presented by Nico Kem, Mercedes-Benz AG

Systems incorporating AI in the Context of ISO 21448 (SOTIF)

With the release of the ISO 21448 ("Road vehicles — Safety of the intended functionality", SOTIF) a fundamental part of how functional safety is defined in other industries has finally been addressed by an explicit standard for the automotive industry which complements ISO 26262. Systems must be free from unreasonable risk - no matter what the root cause of a hazard in E/E systems is: a malfunctioning behaviour or a functional insufficiency.

Innovative systems more and more incorporate AI approaches that aim to improve the overall performance of the intended functionality even in safety related applications. This indicates the special importance of such systems in the context both Functional Safety and SOTIF as one of the main risks of AI applications is the lack of transparency of the corresponding methods.

This talk will point out how the processes defined in ISO 21448 can be utilized to support the creation of a credible safety argument addressing typical risks of AI applications.

Presented by Tim Jones, exida

A Statistical View on Automated Driving System Safety Architectures

This speech discusses the challenges involved in meeting tolerable risk targets for automated driving (AD) functions of SAE L3 and above with current sense-plan-act safety architectures, including sensors.

The evaluation is performed for classes of safety-related driving scenarios. Illustration by fault-trees is used to facilitate understanding by Functional Safety practitioners. It is intended to contribute to the discussion

on how much diverse redundancy of sensors and algorithms is necessary, since diverse redundancy is costly and may increase complexity depending on the fusion strategy. Based on the evaluation of exemplary low

and high frequency safety-critical traffic scenarios, this paper provides evidence that a diverse redundant system consisting of two channels will most likely not meet the tolerable risk target. It shows two consequences.

First, the correlation or common cause failures between sensor measurements needs to be better understood and quantified. Second, extension of the AD architecture by a warning subsystem and in the future V2V communication, as practiced in other industries, may decrease the risk of injury. The quantitative advantage and safety objectives are elaborated.

Presented by Rainer Faller, exida

Sensitivity Analysis within the Prospective Safety Integrity Framework

In safety, dealing with uncertainties is a major concern because many effects can only be described stochastically (aleatory uncertainty) and limited data often requires simplifying assumptions (epistemic uncertainty). Therefore, developers must investigate how sensitive the estimated risk is to uncertainties in the model. This so-called Sensitivity Analysis (SA) involves identifying the most safety-critical components to improve and identifying the critical assumptions to be supported by more evidence. However, the term "Sensitivity Analysis" is not mentioned in ISO 21448, although it is particularly relevant for assessing the risk of performance limitations. The presentation will provide a simplistic example to demonstrate the use of a SA within the Prospective Safety Integrity Framework.

Presented by Prof. Dr. Moritz Werling, BMW Group

Functional Safety with Complex High-Performance Compute Systems

Well-established practices for assuring functional safety exist for traditional automotive systems, but not yet for complex high-performance compute systems required for emerging technologies, such as autonomous driving systems (ADS).

The talk explains why high-performance compute systems are required for ADS, what the challenges regarding functional safety are and how the development ecosystems and operational environments differ from a functional-safety perspective.

The talk then discusses properties of high-performance compute systems that can be leveraged to increase integrity and how redundancy on different levels can be used to increase the systems level of integrity to what's necessary for the intended operation.

Presented by Tilmann Ochs, Argo AI

Differences and Similarities when Arguing Safety and Security

Already at a high-level Safety and Security share one thing: both need argument and evidence. That is, we need to tell a story supported by evidence and references to convince ourselves and others that what we did is sufficient to claim that the final product is safe and secure.

But what happens when we dive deeper? Are the two still similar?

Using Goal Structuring Notation (GSN), the story can be convincingly visualized for functional safety according to ISO 26262 as well as for cybersecurity according to ISO 21434.

This presentation gives insight into similarities and differences based on experience gained during the AUTOSAR basis software development at Vector.

Presented by Jonas Wolf, Vector Informatik GmbH

A systematic approach on defining cybersecurity case to comply with different industry standards – a supplier story

Convincing assurance cases consist of implicit and explicit argumentation. Recent publications already used layers to structure assurance cases for functional safety. We present an evolution of layered assurance case argumentation for cybersecurity relevant components. Benefit: The layered assurance case is less dependent on the structure of a specific standard. Compliance to different standards can be argued more efficiently. This is especially important for suppliers which provide Components out of Context for different application domains. The approach has been successfully applied as a case-study from an IP provider perspective.

Presented by
Debojyoti Bhattacharya / Lucas Bressan, ARM & Clemens Roettgermann, exida

Reliable in-vehicle networks through inline processing of safety mechanisms embedded in networking SoCs

The Software-Defined Vehicle (SDV) paradigm mainly refers to the increasing configurable and customizable features and functions integrable in future vehicles. Such concept, inspired by the proven flexibility of consumer products like smartphones in terms of downloadable and installable apps -that is, functionalities- and their over-the-air (OTA) update, is now aimed to be emulated in modern vehicles.

The future vehicle concept -envisioned as an autonomous and connected cyber physical system transitioning its E/E architecture from domains to zones- makes now much more challenging than ever the design task of deploying functional safety and cyber security countermeasures in it. As consequence of this radical transformation, the in-vehicle network (IVN) becomes an essential part of the vehicle infrastructure and the real enabler of scalable functionalities distributed across the different zonal and/or high-performance controllers and computers allocated there.

The right HW/SW codesign and partitioning of network-related safety mechanisms is identified by the authors as the crucial design aspect in order to succeed in the resolution of this technical problem. Due to the exponential rise of system and software complexity of the vehicle forced by the growing and unstoppable demand of new services and functions, hardware-centric approaches are getting more and more attention to overcome state-of-the-art software-based solutions based on the execution of instructions on multi-core processors deploying algorithms with high-demanding time management requirements. All in all, this talk discloses the strategy followed by the authors in order to develop networking safety mechanisms in next-generation SoC devices embeddable in zonal gateway controllers.

Presented by Dr. Francesc Fons, Huawei Technologies

Soft Errors in Advanced Semiconductors and Automotive Systems

Soft errors contribute considerably to the failure rate of automotive systems, and they may very well be the dominating factor for random hardware faults in advanced semiconductors. And still, much confusion and uncertainties remain in the industry whether and how such transient faults should be considered and analyzed in safety systems. In this presentation we provide an overview how to determine soft error failure rates, what are effective counter measures and safety mechanisms, and how transient faults should be analyzed within a safety related product development.

Presented by Alexander Griessing, James McGinley, exida

A Linux based cybersecurity system for an autonomous platform

The automotive industry and especially BMW is faced with trends and customer wishes, such as autonomous driving, journey management, data sharing, always on, flexible usage models (e.g., sharing, or caring), and interconnectivity, which increases the numbers of interfaces.

The system complexity overruns the complexity of many IT systems, and every unprotected or direct accessible (e.g., from the Internet) interface will be used as attack surface.

In the domain of autonomous driving BMW relies on automotive and open standards with a combination of Adaptive AUTOSAR running upon Linux RT operating system.

The upcoming UNECE regulation (R155, R156, and R157) demands high security standard for autonomous driving platforms.

Satisfying the UNECE expectation and preventing attacks BMW put relatively high level of time and effort in hardening the autonomous platform.

We present a list of methods for securing a Linux system, used as a basis for an autonomous platform, from both external and internal threats by keeping a system up to date, maintaining a secure firewall, and setting strong file permissions.

Presented by Alexander Camek, BMW Group

Is Rust ready for safety related applications?

It is getting increasingly difficult to ignore the advantages of Rust as a language suitable for use in safety related applications. A commercially supported compiler is available with support for several devices already. How difficult will it be to link to existing C libraries, port code from C to Rust, and ultimately construct safety argumentation around mixed language solutions. This presentation will explore the stated advantages of Rust compared to C and the new difficulties that may arise for programmers starting new projects in Rust or converting existing code.

Presented by Jonathan Moore, exida

Improving safety through deterministic construction

For over a decade, Codethink has been troubleshooting system problems, and learning many mechanisms by which the integrity of systems development may be compromised inadvertently by following accepted practices, even within well-defined and controlled processes in the presence of good policy. Our learnings led to the ISO 26262 tool qualification of the Deterministic Construction Service (DCS) reference implementation, leveraging the property of binary reproducibility, pioneered by the Reproducible Builds project (https://reproducible-builds.org), to verify the integrity of the inputs and toolchains used to construct complex safety-critical software components, along with the change management, configuration management, and automated build processes used to control that construction.

By using this reproducibility property, we can:

- Verify that we have control over all of our inputs, including those from supply chains
- Verify that our process is isolated from environmental disturbances
- Avoid unnecessary re-testing or re-validation of unchanged binaries
- Verify the integrity of cached artifacts, which are used to accelerate builds
- Determine whether new toolchain revisions have an impact on previously validated software
- Determine whether other supporting tools have an impact on output binaries
- Use comparison results to inform impact analysis and identify artifacts needing re-validation

We describe some of the practices we have encountered, and demonstrate how this reproducibility property, used as part of a continuous integration workflow, provides organisations with confidence that these issues can be detected. We then illustrate how the benefits listed above can prevent violations of safety integrity and simplify the impact analysis and re-validation of changes.

Presented by Paul Sherwood, Codethink

Building a successful FuSa story: The four Red Hat In-Vehicle Operating System pillars

The claiming of Red Hat In-Vehicle Operating System Safety Profile is ASIL-B-compliant" is based on four high top level safety claims: “Foundation is solid”; “Top Level Safety Requirements (TLSR) are met”; “Process follows ISO 26262” and “Continuous certification is built”. This session provides an overview on our Assurance Management Governance that drives:

- the evaluation of single RPMs as suitable for their use in Red Hat In-Vehicle Operating System product,
- the creation of V&V strategy for showing the compliance with the allocated requirements
- the scoring mechanism model for assessing the applied internal processes against the normative requirements
- the pre-defined and automated infrastructure for implementing the Continuous Functional Safety Certification processes and the updates of Certification Assembly.

Presented by Roberto Paccapeli, Red Hat

An innovative ISO26262-certified architectural OS solution for the Automotive Sector

Last year Red Hat introduced the key pillars driving the certification of the Red Hat In-Vehicle Operating System Safety Certified Profile and the ingredients that Red Hat can leverage along with the development and release pipeline. This session will provide details of the Red Hat In-Vehicle Operating System Safety Certified Profile main architectural features, qualification flow and continuous certification strategy. Details will be provided about:

- the safety scope
- how mixed criticality is supported and the FFI claim
- how FDTI deadline are met
- the functional safety qualification flow
- the continuous certification strategy

Presented by Gabriele Paoloni, Red Hat

Analysis for qualification of complex open-source software

There are various approaches to qualify existing open-source safety-related software. They are not yet well standardized or not easily applicable unless the software is simple. Depending on software complexity, design/architecture, a different approach needs to be selected. For example, you would differently treat a qualification of simple embedded C library, glibc, C++ library and linux kernel or a Linux-based distribution. But in any case, there is a need (in general), to measure the complexity and derive safety measures, safety mechanisms and tests, based on realistic failure modes. This presentation presents an approach for a systematic and efficient approach for safety analysis of such open-source software.

Presented by Piotr Serwa, exida

Bringing innovation into the Automotive Ecosystem - how Red Hat is supporting initiatives and communities

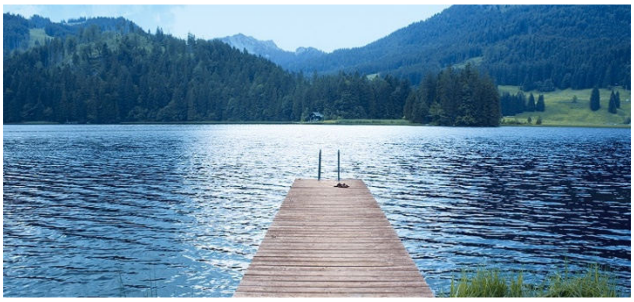
The success of Red Hat is the result of active participation in a huge variety of partners and community projects. This session will provide an overview of the Red Hat active engagements in the Automotive Ecosystem and of how all these engagements contribute to the final success of the Red Hat In-Vehicle OS Safety Certified Profile. More specifically the following aspects will be touched:

- The CentOS Automotive SIG project (how to democratize the code and enable active experimentation and prototype)
- The ISO-PAS 8926 (contributing on "Qualification of Pre-Existing SW product" topic with Safety standard community)
- ELISA (introducing safety into the Linux Kernel community)

Presented by Gabriele Paoloni / Roberto Paccapeli / Harald Ruckriegel, Red Hat

Our Symposium Location

Conferences that offer new perspectives



Hear the stillness. Find tranquility and concentration. This is the ideal place for creative and effective work.

★★★★ Superior
ARABELLA
ALPENHOTEL
AM SPITZINGSEE
Schliersee - Oberbayern

You can expect two unforgettable days full of information, exchange, and impressions at an altitude of 1,100m (3,600ft) in an unmistakable Alpine landscape.

- Wednesday October 12th meet and greet / champagne reception.
- Two nights (October 12th / 13th) in a single room
- October 13th and 14th: two days symposium with food and drinks*

Location: http://www.arabella-alpenhotel.com/how-to-get-there/

*soft drinks, beer, wine, coffee, tea. Other alcoholic drinks will be on your own expenses.

Registration Form ONSITE

I register for the:
***exida* Automotive Symposium 2022**

Date: October 13 and 14, 2022

Location: Arabella Alpenhotel am Spitzingsee
Seeweg 7
83727 Schliersee-Spitzingsee
Germany
www.arabella-alpenhotel.com

Price: € 1,695. -- + tax
The price includes the accommodation.

Please enter the billing address:

Company: ____

Name: ____

Department: ____

Street. ____

Post code, city, country: ____

Email: ____

Phone number: ____

Please send the filled page via email to kerstin.tietel@exida.com.
Booking conditions: The symposium will be held in English and the presentation slides will be in English. In case the registered participant sends a written cancellation 50 day before the start of the symposium the cancellation will be free of charge. Until 21 days before the start of the symposium a cancellation fee of 50% of the fee will be charged. For later cancellations done by registered participants the complete symposium costs will be charged. A replacement of the registered participant with another person is possible at any time. The acceptance of the conditions is part of the registration. *exida.com* GmbH reserves the right to cancel the symposium at short notice and in writing. In this case only the symposium fees will be refunded.

Data protection: The collected personal data is only stored and used for internal purposes related to the management of the training. This data is protected by limited access rights. The duration of the archiving depends on the legal requirements.

____
Date Signature

Registration Form ONLINE

I register for the:
***exida* Automotive Symposium 2022**

Date: October 13 and 14, 2022

Location: Online

Price: € 990. -- + tax

Please enter the billing address:

Company: ____

Name: ____

Department: ____

Street. ____

Post code, city, country: ____

Email: ____

Phone number: ____

Please send the filled page via email to kerstin.tietel@exida.com.
Booking conditions: The symposium will be held in English and the presentation slides will be in English. In case the registered participant sends a written cancellation 14 day before the start of the symposium the cancellation will be free of charge. Until 7 days before the start of the symposium a cancellation fee of 50% of the fee will be charged. A replacement of the registered participant with another person is possible at any time. The acceptance of the conditions is part of the registration. *exida.com* GmbH reserves the right to cancel the symposium at short notice and in writing. In this case only the symposium fees will be refunded.

Data protection: The collected personal data is only stored and used for internal purposes related to the management of the training. This data is protected by limited access rights. The duration of the archiving depends on the legal requirements.

____

Date Signature