How to certify an AUTOSAR operating system

EB's AUTOSAR-compliant EB tresos Safety OS has been certified by exida according to ASIL D and SIL 3. Experts of both companies explain the certification process.

EB (Elektrobit) is one of the first suppliers to offer an ASIL D-certified AUTOSAR operating system. It is also the only system in market to be certified for Safety Integrity Level 3 (SIL 3), the standard for applications outside of the automotive industry. ASIL D and SIL 3 are the highest functional safety standards in accordance with ISO 26262 and IEC 61508 for electrical and electronic components. The Functional safety certification was performed by the independent assessment agency exida Certification SA, which confirmed that the EB tresos safety operating system is suitable for use in Automotive Safety Integrity Level D (ASIL D) applications such as electric power steering. Rainer Faller, Principal Partner of exida, and Robert Leibinger, Product Manager Software & Tools at EB, provide insights into the certification process.

Why should automotive suppliers have their products certified?

Rainer Faller:

Functional safety is a key topic and the products are very complex. As such, all safety standards for higher safety levels require that the development of the products and the applied and documented safety measures must be subject to an independent assessment. Exida assessments also cover technical safety of the product. Certificates are a voluntary confirmation of successful assessments.

The wording of basic functional safety standards such as ISO 26262 is deliberately very general and the respective product categories are open to interpretation. Implementation of the requirements is supported by a large number of documents. In addition to being very time-consuming, assessments require extensive knowledge of the products and standards. They provide the product user with independent confirmation of the safety level achieved. It therefore makes sense for functional safety to be assessed once rather than by each individual user. The applicability of the assessment results must be evaluated by the user for each case, of course.

What should companies such as Elektrobit consider with regard to safety certificates? Are there differences and how can these be identified?

Rainer Faller:

The exact scope of the assessment and the level of detail are important for the user. ISO 26262, for example, also allows assessments of parts of the development. It is possible to perform an assessment of the development processes and measures against the applicable standard requirements without assessing the safety features of the specific product. Assessment statements are also always associated with certain assumptions of which the user must be aware. This key information is contained in the assessment reports and is not evident from the certificate alone. Certificates without meaningful reports thus don't comply with the standards and are not authoritative for users.

EB develops software for two areas: infotainment and ECU. Why was the safety operating system the first product to be certified?

Robert Leibinger:

Compared to most infotainment devices, functions such as brakes and airbags must meet significantly higher safety standards to rule out any danger to road traffic. The relevant ECUs, which perform tasks to the highest "Automotive Safety Integrity Level" (ASIL) D, must therefore be verifiably safe. The operating system is the key component within a safety architecture and forms the basis for all other safety mechanisms implemented in the software. As such, it should also be the first element to be certified.

The influence that the basic components of the operating system can have on the ECU as a whole should not be underestimated. The operating system is not just responsible for memory partitioning but also for controlling the entire program flow including safety mechanisms. For this reason, EB already decided more than two years ago to develop a new kernel, optimised solely for safety. Rather than incorporating additional features into an existing system, this new concept was designed from scratch. The requirements, design, implementation and tests were all geared towards functional safety. From the outset, the aim was to develop a reliable safety operating system that could be integrated seamlessly into AUTOSAR.

A product can be certified in many different ways. How does exida approach this task?

Rainer Faller:

Our assessments look at both the development processes and the product's technical safety features. The assessment takes place in multiple stages. Once the scope of the assessment has been agreed upon, the implementation of the safety specifications is assessed based on the documentation – independent of the product managers, developers and testers. Any questions that arise are clarified in meetings and the practical implementation of the processes and procedures defined by the manufacturer are scrutinised in a manufacturer audit.

The assessment takes into consideration all relevant ISO 26262 objectives and work results. The starting point for the assessment is the safety case provided by the manufacturer and the development documents referenced therein. As the objectives are very general, the assessor selects other key standard requirements. At exida, this is supported by a safety case database tool which also contains coordinated interpretations. When selecting requirements from the product's technical requirement specification, particular consideration is given to the safety features, fault detection measures and error responses which are important to the user. These are described in the assessment report.

How was the cooperation between exida and EB?

Robert Leibinger:

The cooperation was extremely constructive. We began by carrying out a joint "pre-assessment" which involved examining the strategy for the development of the Safety OS in more detail with regard to functional safety as well as plans and requirements. This enabled us to incorporate the assessment requirements in our development process at a very early stage.

In the next step, we identified the technical scope of the certification, i.e. which operating system functions were relevant in terms of safety and therefore needed to be assessed. These functions then form the basis for a "Safety Element out of Context" on which our customers can develop their safety rationale. Using these data, exida was then able to create an assessment plan which defined the nature and scope of the certification process.
Only then did we begin the actual assessment, holding regular joint meetings and intense debates. All relevant topics, including the implementation of the requirements, design and tests, and the source code were examined at a highly technical level. In addition to the process evaluation, we also considered the architecture and the implementation of safety aspects for the operating system.
Aside from the assessor, Rainer Faller, the assessment meetings also involved the EB Safety Manager and all development, test and quality engineers assisting in the development of the operating system. Given the wealth of material available, it was a huge challenge to prepare the necessary information in the appropriate form in order to support the rationale. Developing the operating system with a view to ensuring functional safety from the outset was extremely helpful.
The assessment report was produced in an iterative process and completed at the end of 2012.

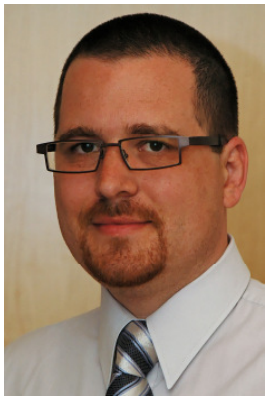
Operating systems such as the EB Safety OS provide the basis for ECUs that have to comply with the highest safety standards. How can the certification of the operating system help with the certification of these ECUs?
Robert Leibinger:
Based on the operating system, safety mechanisms are implemented which must meet the highest safety standards. These mechanisms must be able to rely on certain basic functions. The exida certificate guarantees the ECU manufacturer that these functions have been checked to the highest standards. If the ECU safety assessment is performed by the ECU manufacturers, they can refer to the certificate when verifying the safety features of the operating system in accordance with ISO 26262. No further measures are required to ensure the basic functionality of the operating system and the manufacturer can exclude this verification from the overall ECU test. To a certain extent, we share the work with our customers by taking over responsibility for verifying the basic functionality of the system.

Rainer Faller:
The guaranteed safety features of the Safety OS are extremely helpful. Protection for the implementation of concurrent software features and logical partitioning, and for the secure processing of the µC configuration during start-up is particularly important for the targeted development of safety-related software. The Safety OS achieves this by combining hardware functions such as memory with hardware resource protection (freedom from interference). The Safety OS thus provides the basis for implementing the logical architecture which is specified by the functional and technical safety concepts in accordance with ISO 26262. This includes both the application software and the AUTOSAR-compatible basic software.

What added value does the certified operating system offer customers?
Robert Leibinger:
Our customers can focus entirely on their core competencies. We provide them with the basic functions for their software in our operating system in accordance with ASIL D. In addition to secure context switching, we offer safety-related functions such as task scheduling, event handling and locking mechanisms. AUTOSAR systems rely on these mechanisms via the RTE, often without the user knowing. Furthermore, this allows these functions to be used directly in the safety mechanism in order to decouple parts of the software via events or to prevent mutual access to shared resources. Our aim was to cover all basic functions with the certificate. This ensures the reliable development of ECUs to the highest safety level.
When selecting the safety-relevant functions, we decided to only include the basic functions in the certification. We wanted to keep the complexity of the software to a minimum in order to make the safety analyses as simple as possible. We also managed to design the non-certified elements through a skilful architecture without influencing the remaining functions. The Safety OS thus offers reliable safety functions while also being AUTOSAR-compatible.

What are the future plans at EB in terms of functional safety?
Robert Leibinger:
Aside from the pure operating system core, further components are required in the development of safety critical software, e.g. program flow control and secure communication. For this reason, here at EB, we are also focusing on having our other products from the EB tresos Safety product family certified in order to offer a complete and independently verified safety package. Our solutions for the safe handling of the runtime environment (EB tresos Safety RTE), protected timing and execution supervision (EB tresos Safety TimE Protection) and the protected transmission of safety-related data between multiple ECUs (EB tresos Safety E2E Protection) will soon also be certified by exida.

Rainer Faller
Principal Partner of exida



Robert Leibinger
Product Manager Software & Tools at EB