ANSYS

White Paper

Analysis and Development of Safety-Critical Embedded Systems: The Need for an Integrated Toolkit

Today's automobiles and airplanes feature more electronic components than ever. Hundreds of connected systems enable safety-critical functions like braking, acceleration, steering, navigation and communication. Underlying all these functional systems are millions of lines of embedded software code that ensure their reliable operation under a broad range of conditions.

With human lives at stake, two engineering teams work to ensure that these mission-critical systems perform flawlessly in the field. One team works to integrate the dozens of components that are brought together in a connected system, ensuring that signals and controls are seamlessly combined in a way that optimizes not only each component but the entire electronics architecture. A second engineering team performs an equally important task: ensuring the functional safety of these components, as well as the overall system. These safety engineers look at the risks, sources and consequences of system failure, in an effort to eliminate risks and maximize resilience to the greatest extent possible.

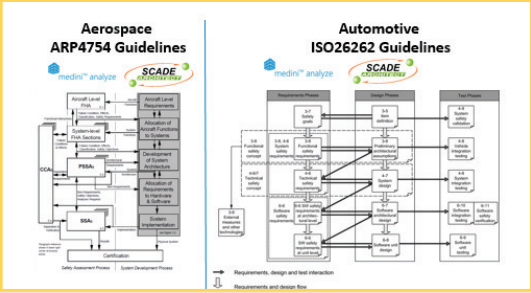
As they work to secure regulatory approvals and ensure safe, reliable operation in the field, these two engineering teams both conduct rigorous modeling, analysis and verification — accounting for each other's activities and making sure all components work seamlessly and safely together.

To make their jobs easier, what's needed is an integrated toolkit that enables system modeling, safety analysis and verification. Such a toolkit would ensure that teams work together in an optimal manner, while eliminating outdated, manual methods for conducting modeling, analysis and verification. Not only would an integrated toolkit save time and money, but it would also increase the accuracy and reliability of electrical software-based systems for cars and planes.

Automotive and aerospace systems feature an incredible number of electronic components that deliver smart functionality. Autonomous electronics and sensors monitor conditions and control every activity within the vehicle — from mission-critical capabilities like braking and steering to "extras" like entertainment technologies. These advanced systems and components are sourced from different suppliers, but must be brought together under a single system architecture that is capable of meeting safety goals. As the number of systems and components increases, it becomes more challenging to monitor and control them, as well as ensure that they will work together in a reliable, consistent manner.

Analysis and Development of Safety-Critical Embedded Systems: The Need for an Integrated Toolkit

Embedded Systems Safety Analysis standards follow parallel tracks...



ANSYS SCADE and medini analyze both offer a model-based, step-by-step approach for developing a reliable system architecture that meets stringent regulatory standards. These solutions work together to create a comprehensive modeling toolkit for software engineers.

ANSYS SCADE has set the standard in the global aerospace and automotive industries for automated generation of both system architecture and embedded software code. SCADE's proven, step-by-step method for modeling a robust control system architecture ensures that all critical components that govern braking, steering and other functions work together seamlessly and reliably. Software engineers can work quickly and efficiently to generate mission-critical code, with the assurance that they will meet both regulatory standards and project deadlines.

The medini analyze software, also offered by ANSYS, automates the modeling and verification of functional safety for automotive and aerospace electronic control systems. Similar to ANSYS SCADE, medini analyze provides a step-by-step modeling and verification process that results in a system architecture that accounts for the safe, reliable interactions of dozens of components. Using medini analyze, engineers can automate the analysis of failure modes, their likelihood and the response of the overall system under a wide range of operating scenarios.

By using these two specialized modeling tools together, for the first time engineers in the aerospace and automotive industries have a single, integrated toolkit. The same reliable, step-by-step process will ensure the creation of system architectures that meet all relevant industry standards for safety and control — quickly and cost-effectively.

A team of systems engineers is tasked with integrating these components and creating a robust architecture that delivers this reliable operation. They must meet strict regulatory standards that are specific to the global automotive and aerospace industries, while also working as efficiently as possible to keep pace with product launch deadlines.

In parallel with the development of the architecture of the system, another team of engineers evaluates and assesses the overall system model for functional safety, which means assessing the dozens of mission-critical components, like braking systems, that underlie every car and every plane. These sophisticated electronics have been well engineered, but can be prone to failure under certain circumstances. Functional safety experts look at the system architecture and identify the potential modes of failure, the likelihood of each event and the response of the entire electronics architecture should this occur. This thorough analysis helps minimize the risk of system failure and meets the stringent regulatory standards for the global automotive and aerospace industries.

When a change is made in the overall system architecture, that change must be reflected in the models of the functional safety team, and vice versa. This can result in slow-moving, ongoing hand-offs as the system architecture is continuously tweaked during the development cycle. Currently, the majority of safety-related activities are conducted either via outdated, manual processes in generic tools like Excel™ spreadsheets (which do not produce reliable results because they were not specifically created for this purpose) or in point tools for specific safety analysis methods that are not well integrated with the rest of the engineering tool set. In addition, manual processes consume time and financial resources, while being prone to error.
With so much riding on the complex, mission-critical electronics systems installed in cars and planes, there should be a better way.

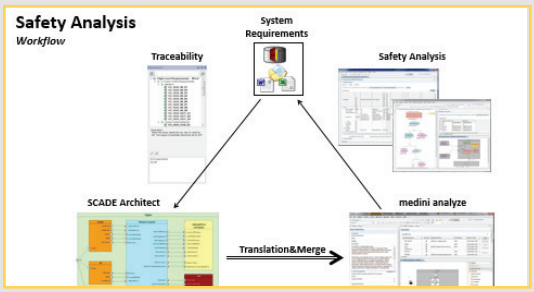
Needed: Specialized Tools That Work Together

Engineers in the automotive and aerospace industries require a comprehensive, integrated toolkit that enables them to design a robust system architecture — and ensures the functional safety of the components under a wide range of operating conditions and parameters.

This toolkit, developed by a recognized industry leader with expertise in both areas, would eliminate manual processes and the significant possibility of human error. Today, as changes are made in one component or the overarching system architecture, these tweaks must be reflected across hundreds of components and associated inputs in that system. Then these updates must be manually handed off to the safety engineering team to ensure that the integrity and functional safety of the overall automotive or aerospace system are maintained.

Analysis and Development of Safety-Critical Embedded Systems: The Need for an Integrated Toolkit

Better Together: SCADE Architect and medini analyze



Any changes in system architecture are easily and seamlessly translated from SCADE Architect to medini analyze. This tight integration eliminates the possibility of human error as electronics systems are modeled, verified and updated.

By leveraging SCADE for control system design and medini analyze for functional safety analysis, for the first time engineers can utilize a shared toolkit and common workflows when working on automotive and aerospace electronic systems.

Any changes in the overall system design are immediately and automatically reflected in the work of functional safety analysts. And, as safety risks are identified by medini analyze, these are addressed in the overall system architecture. Instead of relying on manual hand-offs and quality checks, the two engineering teams can benefit from a reliable and accurate set of software tools created specifically for this task, offered by industry leader ANSYS.

SCADE and medini solutions also integrate tightly with the full suite of ANSYS solutions for engineering simulation and the ANSYS platform. Whatever their specific challenge, automotive and aerospace engineering teams can rely on ANSYS for proven software solutions that have been successfully leveraged by more than 45,000 customer organizations worldwide over the past 40 years.

With hundreds of components and inputs — and ongoing updates to them — there is a significant possibility of human error if engineers are relying on manual processes and generic desktop tools like Excel to manage these changes. The pressure to work quickly to launch a new car or plane only adds to the risk of making a mistake.

With an automated, integrated system modeling toolkit, a single change would immediately and automatically be verified across the entire system architecture, ensuring flawless operation of that system. Both system-level and functional safety engineers could be confident that any changes they make are reflected by the other team, and that all regulatory standards for performance and safety are being met by the system design. No human intervention would be required to make universal changes, flag any performance issues and generate a reliable system architecture supported by flawless embedded software code.

The Benefits of an Integrated, Step-by-Step Approach

The process of designing, analyzing and verifying a system architecture for automotive and aerospace electronics might be complex — but, in the end, it is a step-by-step, repeatable process that can be managed by the right software tools. By automating the many steps, decisions and risk analyses involved in this process, architecture design and verification can be made much more accurate and comprehensive, taking into account every component, input and interaction.

An automated, integrated toolkit for designing a robust system architecture — as well as ensuring its functional safety — would deliver a number of benefits. These include:

- Increased consistency because all involved engineering teams would be working with the same toolkit, processes and workflows — leading to predictable, repeatable design methods and results

- Improved quality and accuracy of system architecture design as an intelligent, automated toolkit would eliminate the possibility of human error

- Faster time to market as time-consuming, labor-intensive modeling and verification activities would be automated and accelerated

- Lower financial resource demands because the engineering staff would be working more productively and engineers would be free to work on higher-value, more strategic tasks

- Enhanced traceability resulting from the fact that, from requirement definition to verification, every activity would be captured and tracked in the toolkit

There's no doubt that it is difficult for engineering organizations to let go of outdated methods and tools that they have relied on for years. However, it would simply make sense for engineers to embrace an automated toolkit that's designed specifically for their design and verification activities — and delivers this wealth of benefits not just for the engineering team, but for the entire business.

Built-In Regulatory Compliance

With the rise of advanced electronics, sensors and smart functionality, automotive and aerospace electronic systems are incredibly sophisticated. Because human lives are at stake, the automotive and aerospace industries have rightfully defined very stringent standards that govern the design and operation of these systems. Engineers must build system architectures that include many levels of checks and redundancies to achieve applicable safety goals, as defined by regulatory standards such as ARP4754 for aerospace and ISO 26262 for automotive applications.

The already complex task of designing a system architecture — and verifying its functional safety — is made much more challenging when engineers also need to understand the many nuances of securing regulatory approvals. By leveraging an engineering toolkit that's designed specifically with these regulatory requirements in mind, engineers can be assured that they are building in compliance at every step. An intelligent toolkit would walk them through a compliant, step-by-step process and flag any exceptions to ensure that all standards for performance and functional safety are being met.

At the end of the process, this intelligent tool would simply produce all the system documentation required to pass regulatory approvals in the automotive and aerospace industries — for both performance and functional safety. Engineers would not have to scramble to justify their system architecture by producing lengthy, time-consuming manual reports.

Leverage the Experience of a Leader

An industry leader in electronic systems design and verification has much to offer engineering teams in the automotive and aerospace industries. Backed by deep experience in supporting engineering teams, a proven leader understands and addresses the complexities of system architecture design, functional safety analysis, verification and regulatory compliance.

Any integrated solution for aerospace and automotive control systems should be developed and supported by an industry leader, in order to deliver the greatest value. The engineering teams should have access to a broad suite of products specifically for system architectural design, embedded software design, system modeling and verification, and functional safety analysis — as well as references from satisfied customers in the automotive and aerospace industries who have already benefitted from this family of solutions.

In addition, it would be helpful if the toolkit developer offered complementary solutions for multiple applications in automotive and aerospace engineering — such as mechanical, fluids and electromagnetic simulation. This would provide companies with a broad product suite to answer all their engineering challenges, from a single provider with proven leadership. Various engineering teams could collaborate more easily, and software tools would be built on a common platform for easy, seamless integration of common engineering tasks.

Realizing Game-Changing Results

An integrated toolkit for designing and verifying the safety of electronic systems architectures would be a game-changer for engineering teams in the automotive and aerospace industries. With so many advanced electronics in today's cars and planes — and with human lives at stake — engineers simply can't afford to rely on outdated manual processes and tools for guaranteeing the safe performance of electronic control systems.

It's never easy to make a change and abandon "the way we've always done things." But, as electronics become smarter and more sophisticated, engineers must adopt an equally sophisticated toolkit to manage and control these electronics.

By capitalizing on a specialized, integrated toolkit that can automate all their system design, functional safety analysis and regulatory compliance activities, engineers can support the overall success of their business in the highly competitive automotive and aerospace industries. They can cut time and costs from the development cycle, leading to extremely rapid product launches — without sacrificing the safety or integrity of the embedded system that forms the foundation for today's smart automobiles and airplanes.

Summary

It's time for engineering teams in the automotive and aerospace industries to stop relying on processes and tools that are clearly outdated — and fail to measure up to today's complex challenges. Just as electronics inside cars and planes have become incredibly sophisticated, engineers must capitalize on technology advances and innovations to manage the mission-critical tasks of designing robust system architectures and ensuring their functional safety under a broad range of conditions.

Just as every technology inside automobiles and airplanes has evolved dramatically in the last decade, engineers must also embrace the new-generation tools that can automate the generation and verification of robust, safe system architectures. With a new, integrated toolkit on the horizon, offered by a proven industry leader, the time has come for engineering teams to match the smart features of their company's products with smart engineering tools and processes that deliver accurate, reliable results at a fraction of traditional time and cost investments.

ANSYS

Analysis and Development of Safety-Critical Embedded Systems: The Need for an Integrated Toolkit

ANSYS, Inc.
Southpointe
2600 ANSYS Drive
Canonsburg, PA 15317
U.S.A.
724.746.3304
ansysinfo@ansys.com

If you've ever seen a rocket launch, flown on an airplane, driven a car, used a computer, touched a mobile device, crossed a bridge or put on wearable technology, chances are you've used a product where ANSYS software played a critical role in its creation. ANSYS is the global leader in engineering simulation. We help the world's most innovative companies deliver radically better products to their customers. By offering the best and broadest portfolio of engineering simulation software, we help them solve the most complex design challenges and engineer products limited only by imagination. Visit **www.ansys.com** for more information.