SOLUTION OVERVIEW

Improving Cybersecurity for Automotive Electronics Systems via Ansys medini analyze

The digitalization of the automobile has delivered a host of benefits — from better safety features to enhanced comfort. At the same time, the increased amount of software in cars, and their greater levels of internal and external connectivity, have made automobiles vulnerable to cyberattacks. Some well-documented examples have demonstrated the real potential for hackers to override automotive software systems and interfere with the safe operation of a single car — or even a fleet of cars. How can the developers of automotive electronics ensure that their systems are secure? Today Ansys medini analyze, a proven solution for ensuring the functional safety of automotive electronics, includes new capabilities for verifying system-level security. By relying on medini analyze, automotive systems engineers can deliver the highest possible level of cybersecurity to their OEM customers, as well as drivers around the world.

Executive Summary

The automotive industry has benefited from the digital revolution, offering consumers a host of new features and benefits enabled by electronics. However, with the increasing electrification and connectivity of cars has come an increasing risk of cyberattacks. With recent headlines focusing on automotive hacking, and a new industry standard for cybersecurity debuting in 2020, it's time for automotive electronics engineers to get serious about cybersecurity. Fortunately, there is a new, advanced solution to help them identify and address vulnerabilities and threats in their systems and components. Ansys medini analyze for Cybersecurity is an easy-to-use modeling and analysis tool that ensures the electronics architecture, with its many connections and interfaces, is impervious to external attacks. By replacing their outdated tools and manual processes with the speed and automation of medini analyze, automotive electronics engineers can deliver safe and secure products, reduce time-to-market, maximize profit margins and comply with upcoming regulations surrounding cybersecurity.

Digitalization: Driving Significant Benefits — and Risks — for Car Owners

Today's smart, connected automobiles are loaded with digital systems and embedded software. As cars become more autonomous, this trend is only picking up speed. The digitalization of automotive design has not only made cars safer and more efficient, but has delivered a range of benefits such as increased comfort, easier navigation and expanded infotainment options.

However, these improvements have not been achieved without a certain degree of risk. According to McKinsey, software lines of code per vehicle have increased from about 10 million in 2010 to about 150 million by 2016 — a 15X increase in just six years.[1] With every exponential increase comes an associated exponential increase in the risk of a software code flaw, as well as an integration error in the overall system design.

Thankfully, technology solutions from Ansyshave helped software developers produce reliable code, as well as support engineers in modeling and analyzing the functional safety of automotive systems, to ensure that integrated electronics will work as expected under a range of conditions.

Recently, headlines have focused on an additional risk factor: With their growing number of interfaces and connections, automotive electronics systems may be vulnerable to hacking by cybercriminals. The levels of security built into the bus technology underlying automotive systems (e.g., CAN) is very basic, leaving them vulnerable to interference. In addition, today's Vehicle-to-Everything (V2X) connectivity has created a complex technology ecosystem with many points of entry for potential cybercriminals.

Increasing Cybercrime Means a New Roadmap for Systems Developers

How real is the threat of automotive electronics hacking? In 2015, in a well-publicized incident, a group of expert hackers were able to gain control of an SUV via its entertainment system and cut the transmission, interfering with basic functions like acceleration. This incident revealed a vulnerability in nearly 500,000 vehicles, causing the OEM to send a security fix to every owner of that model.

In 2018, researchers at Keen Security Lab in China identified at least 14 electronics-system vulnerabilities in luxury car models, which they reported to the automaker. And, demonstrating the vulnerability of every make and model, in 2019 an anonymous hacker was able to access the controls of over 27,000 cars simply because their owners were using the default password on their GPS navigation apps.

Who is responsible for designing electronics systems that are safe against these kinds of sophisticated attacks? That job falls to automotive electronics engineering teams, which work to integrate dozens of digital components — including navigation and infotainment, but also braking and other critical functions — and ensure they are brought together in a securely connected system. These engineers must ensure that signals and controls are seamlessly combined in a way that optimizes and safeguards not only each component, but the entire electronics architecture.

Already overwhelmed by the sheer volume of digital components and the complexity of system-level architectures, these engineers are now charged with identifying, and addressing, every possible vulnerability. They need to model the entire electronics architecture — including every interface, control and connection — to ensure that the vehicle and its systems will be protected from malicious hacking attempts.

To guarantee that automotive electronics engineers are doing an adequate job, a new ISO standard is being developed for system-level security. Similar to ISO 26262, which governs the functional safety design of road vehicles, ISO 21434 will ensure that engineers have arrived at a secure electronics architecture — and have documented all their modeling and verification activities.

Recent headlines, as well as the new ISO 21434 standard planned for November 2020, are placing unprecedented pressures on electronics engineers in the auto industry. Traditional workflows and generic tools like Excel™ spreadsheets are proving inadequate in meeting these new demands. What's needed is a new modeling solution and an associated set of best practices designed specifically to meet the growing cybercrime challenge.

[1]https://www.mckinsey.com/industries/automotive-and-assembly/our-insights/rethinking-car-software-and-electronics-architecture

Managing the Risk: Introducing Ansys medini analyze for Cybersecurity

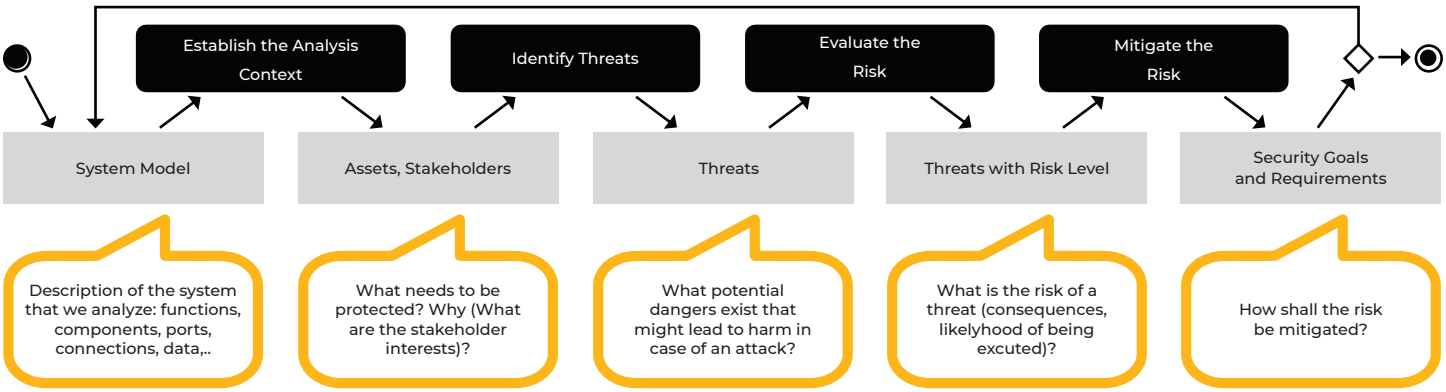
Fortunately, today electronics system engineers have a new weapon in the fight against cybercrime: Ansys medini analyze for Cybersecurity. Offered by engineering simulation leader Ansys, this specialized modeling solution streamlines and accelerates the complex task of generating and verifying a cohesive, safe, secure, system-level architecture that is impervious to outside attacks.

For years, functional safety experts have leveraged medini analyze to study the over-arching electronics system architecture and identify every potential mode of failure, the likelihood of each event, and the response of the entire electronics architecture should this occur.

Now automotive systems engineers have a new tool available to streamline and accelerate their cybersecurity assessments — replacing outdated processes that rely heavily on manual labor and error-prone human analysis. Ansys medini analyze is a customized solution designed to replace consumer-grade software tools, notably Excel™, which were not designed to organize and facilitate the analysis of highly complex electrical systems.

Not only are today's manually intensive processes and generic software error-prone, but they are inefficient — which means automakers could be slow to market with their new cyber-safe system designs. In today's fast-moving world, OEMs and consumers simply can't afford to wait to protect their vehicles against hacking attempts.

How exactly does Ansys medini analyze for Cybersecurity work? Across the entire electronics architecture, medini analyze carries out this six-step process aimed at identifying and addressing cyber vulnerabilities:



- Identify the assets inside vehicle systems such as braking, steering, lighting, HVAC, GPS navigation and infotainment systems
- Discover the system-level vulnerabilities, such as interfaces, that place these assets and their performance at risk
- Understand the consequences of exploiting these vulnerabilities, at the system and component levels
- Estimate the potential likelihood of an attack, based on the effort needed to execute it
- Define a risk level for each threat by calculating both the likelihood of an attack and the potential consequences
- Plan and execute appropriate cybersecurity measures to guard against all identified risks, beginning with the highest-level risks

In conducting this analysis, Ansys medini analyze for Cybersecurity assesses a wide range of attack scenarios, then determines potential risks that might occur in these scenarios. New capabilities in medini analyze for Cybersecurity facilitate the process of looking at the overall electronics architecture, as well as each digital component such as infotainment. Engineers can quickly identify vulnerabilities and design weaknesses, then address them to mitigate any real-world hacking attempts.

Engineers can leverage Ansys medini analyze for Cybersecurity to ensure they are neither under-estimating actual risks or over-engineering their systems, which wastes precious time and money. They can achieve an optimal level of cybersecurity by looking at realistic attack scenarios and the level of control each can exert over the vehicle and its many electronics systems.

Because experts at Ansys understand the regulatory complexities of ISO 26262 and the upcoming ISO 21434 cybersecurity standard scheduled to debut in 2020, Ansys medini analyze for Cybersecurity is designed to address these system-level design requirements. In addition, medini analyze for Cybersecurity automatically generates the documentation required to verify the security of all electronic systems to automotive regulatory groups and OEM customers.

While medini analyze for Cybersecurity is a new solution, some pioneering medini customers are already applying the software for cybersecurity assessments.

/ Reduce Your Exposure — and Increase Your Profits

Ansys medini analyze is a customized, cost-effective solution to ensuring the cybersecurity of complex automotive electronics systems. By relying on medini analyze, engineering teams can realize these benefits:

- A much lower risk of damaging cyberattacks. By identifying every possible means of cyberattack — and estimating both their impact and their probability — systems engineers can minimize the potential risk of being attacked. They can confidently deliver electronics architectures to OEMs and customers worldwide, with the knowledge that they have systematically studied and reduced risk exposure.
- Compliance with customer needs and upcoming industry standards. Developed by the experts at Ansys, medini analyze for Cybersecurity meets customers' expectations for secure, verified system design. It also anticipates the upcoming ISO 21434 standard for automotive cybersecurity, set to be announced in November 2020. The Ansys medini analyze team will continue to monitor the progress of this standard as it is defined. In addition, medini analyze for Cybersecurity simplifies the process for documenting the system modeling and verification process, so proper documentation can quickly and cost-effectively be submitted to customers and regulators.
- A significantly faster development process. Manually modeling the system-level electronics architecture, and identifying vulnerabilities and potential attacks, via consumer-grade software tools is a tedious, labor-intensive effort that's slow — and also prone to mistakes. Instead, medini analyze for Cybersecurity follows a step-by-step, efficient process that eliminates the chance of human error. Engineering teams can work faster, more accurately and with a much higher level of productivity. The use of medini analyze delivers significant efficiency benefits and supports a much shorter development cycle, for faster time-to-market.

- Lower costs and higher profits. By eliminating a large part of the manual analysis involved in cybersecurity assessments, Ansys medini analyze can significantly cut development costs. Fewer staff members can accomplish more by relying on this modeling based tool to streamline and accelerate common analysis tasks. In addition, Ansys medini analyze for Cybersecurity creates a repository of information, such as typical attack types, that can be re-used for multiple analyses. Engineering teams can support higher profit margins via both reduced development costs and the introduction of more innovative electronics system designs.
- Synchronization with other leading solutions in the Ansys software suite. Ansys medini analyze for Cybersecurity seamlessly integrates with other leading technology solutions for electronic systems design, including the SCADE family of solutions for embedded software development. By relying on a common technology platform and shared interfaces, the entire engineering team can benefit from enhanced collaboration, transparency and visibility.

Attack Your Competition via a Smart Cybersecurity Strategy

Due to well-publicized hacking events, the automotive industry is becoming more aware of the crucial importance of cybersecurity. The upcoming ISO 21434 standard will force every OEM and electronics system provider to consider cybersecurity as part of the product development process. Consumers around the world are also beginning to question, “How safe is my vehicle from a remote attack?”

In this environment, early adopters of innovative cybersecurity measures can assume a meaningful competitive edge. Backed by the proven performance of medini analyze for functional safety — and the historic technology leadership of Ansys— medini analyze for Cybersecurity is an obvious choice for those electronics engineering teams looking to increase their focus on cybersecurity analysis.

While the automotive industry is an early target for cybersecurity analysis, many other types of businesses can enjoy these benefits as they apply Ansys medini analyze for Cybersecurity to their own development challenges (see sidebar, “Looking Beyond the Automotive Industry.”)

Hackers are getting more and more sophisticated, as they explore new ways to override vehicle safeguards. But one thing is certain: Those companies implementing advanced tools and best practices in the war against cybercrime will emerge as the winners.

The solution is Ansys medini analyze, already used by the world’s leading electrical engineering teams to automate the complicated process of functional safety analysis. With its new capabilities for cybersecurity, it delivers the global automotive industry’s most comprehensive toolkit for system-level analysis that supports the safe, reliable performance of millions of vehicles around the world.

Looking Beyond the Automotive Industry

Ansys medini analyze for Cybersecurity is already being utilized by electronics development teams in the global auto industry. But companies in other industries can also enjoy this solution’s fast, efficient, accurate approach to identifying and addressing cyber threats.

For example, aerospace and defense companies face an incredible amount of pressure to safeguard their assets, in both military and civilian applications. Just as in the automotive industry, hacking can endanger human lives and result in financial damages — and the stakes are extremely high when there are hundreds of passengers aboard a single airplane.

Similarly, the maritime industry — which includes both military and commercial craft — could be a target for cybercrime. With shipping lanes covering thousands of miles of international waters, the repercussions of a single successful attack could be devastating.

From oil rigs and nuclear plants to smart grids, the global energy industry is also vulnerable to acts of cyber sabotage. And imagine the enormous impact if cybercriminals were able to hack into common consumer electronics such as phones, laptops or home security systems.

In these industries, and more, Ansys medini analyze for Cybersecurity could be incorporated into product engineering processes to create a new level of confidence and safety.

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.