DevSecOps in the Automotive Sector

The Essential Practice for Automotive Security, Safety, and Customer Trust

WNDRVR

As Software Becomes Ubiquitous in Vehicles, Security Is Paramount

Bolt-on solutions are no longer adequate to the challenge of ensuring vehicle security. Best practices now embrace the principles of DevSecOps, embedding protections at the earliest stages of development and providing long-term automated testing.

$10.5 trillion

The annual cost of cybercrime by 2025[1]

— Cybercrime Magazine

Vehicle manufacturers and independent software vendors developing automotive solutions are increasingly adopting DevSecOps practices to bolster security protections and add to the safety of vehicle operations. Assessing and eliminating potential vulnerabilities as an integral part of the design during the early stages of development leads to more secure solution releases and more effective code maintenance.

DevSecOps, which is a natural extension of familiar DevOps practices, automates tasks and brings consistency and structure to code development. Frequent code releases and reviews, security monitoring, and simulations are used to identify risk factors and alleviate them during development and as part of an ongoing maintenance regimen. As autonomous and semiautonomous vehicles begin to fill the roadways, the increased security DevSecOps promises is vital to ensuring customer trust, meeting rising cybersecurity challenges, and improving driving safety.

[1] *cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016*

What Is DevSecOps?

The DevSecOps process evolved from DevOps, which combines software development and operations into a unified process with a cyclical flow.

This cycle relies on rapid releases of code, vigorous testing and feedback, and awareness of the full lifecycle of the software product. Broadly adopted by many organizations as a fundamental and useful set of practices to guide software builds and updates, DevOps has evolved into DevSecOps, adding security provisions into the cyclical flow, as shown in Figure 1. Code planning, building, testing progress, and security issues — including threat mitigation, scanning, analysis, remediation, and ongoing monitoring of each release of the code — are examined as part of the cycle.

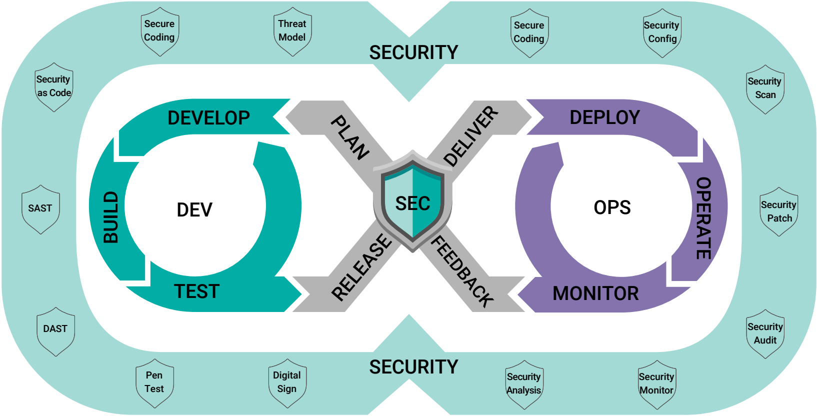
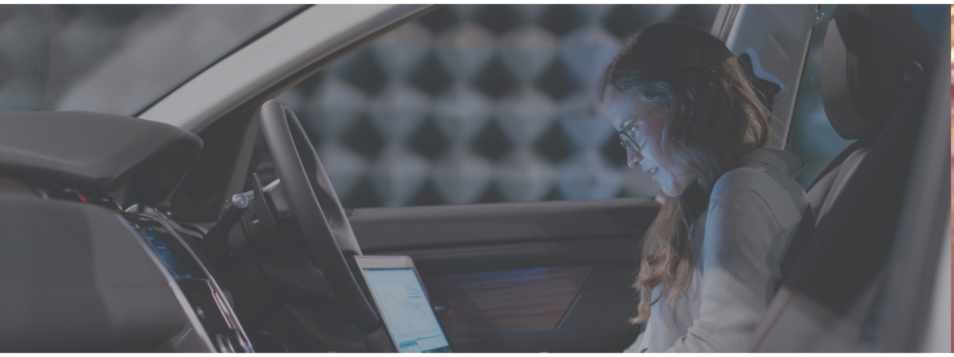


Figure 1. DevSecOps adds security to familiar DevOps practices

> “As a result of the overarching cybersecurity concerns in modern automobiles, the United Nations Economic Commission for Europe (UNECE) recently developed two new regulations on cybersecurity and software security designed to help manage the risks moving forward for both manufacturers and consumers.”
>
> — SecurityBoulevard.com

Vehicle security protection is paramount in two main areas: the design and use of electronic control units (ECUs) and automated driver assistance systems (ADASes). The repercussions of a vehicle’s ECU or ADAS being hacked or controlled externally by someone other than the driver could be extreme, in terms of both safety and personal privacy.



Organizations tasked with protecting transportation systems and the public welfare are becoming proactive in addressing risk factors. For example, writing for Security Boulevard, Stephen Gates states:

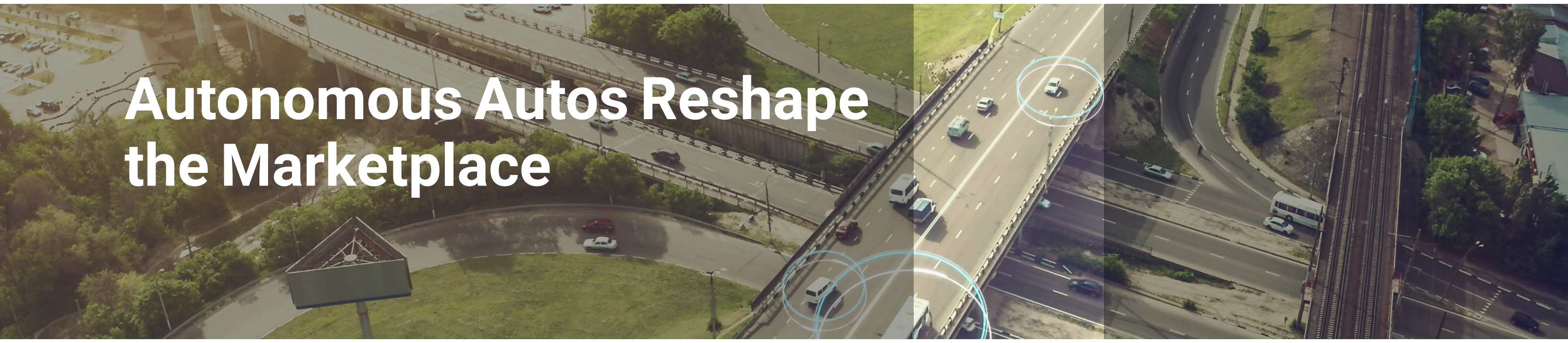
> *"As a result of the overarching cybersecurity concerns in modern automobiles, the United Nations Economic Commission for Europe (UNECE) recently developed two new regulations on cybersecurity and software security designed to help manage the risks moving forward for both manufacturers and consumers. The binding regulations are the first-ever globally coordinated effort in the area of automobile security. The regulations will apply to passenger cars, vans, trucks, and buses and they will enter into force in January 2021. These regulations are primarily being driven by the fact that today's automobiles can include 150+ electronic control units (ECUs) and roughly 100 million lines of software code, which is estimated to be about 4x more than a modern fighter jet."*[2]

> "By 2023, more than 775 million cars will be connected by means of telematics or in-vehicle apps (compared to 330 million in 2018)."[3]
>
> — Juniper Research

Expectations are that similar kinds of regulatory mandates will begin appearing at national and international levels as automobiles, trucks, and other vehicles become rolling software platforms. Wind River® has been an early participant in efforts to enhance vehicle security and is a trusted solution provider with an extensive record of delivering embedded security solutions resistant to cyberattacks.

In the U.S., the National Highway Traffic Safety Administration provides guidance to manufacturers and system developers in the automotive space to assist in the creation of automated driving systems (including safety standards), recommended laboratory testing, the use of simulations, and education. A report describing its perspective, *Ensuring American Leadership in Automated Vehicle Technologies*, was issued in January 2020.

[2] securityboulevard.com/2020/07/on-the-road-to-devsecops-securing-the-software-driving-mobility
[3] www.juniperresearch.com/press/press-releases/in-vehicle-commerce-opportunities-exceed-775mn



Autonomous Autos Reshape the Marketplace

Safety systems and security protections must keep up with the proliferation of autonomous vehicles.

The global autonomous vehicle market is expected to escalate at an annual growth rate of 39.5%[4] between 2019 and 2026. With the magnitude of this leap in automotive complexity, there exists a corresponding need for embedded safety and security mechanisms. Given this set of conditions and the rapidly changing environment, the value of DevSecOps is amplified substantially. A system must be in place to accommodate the technologies and systematically provide for software updates and patches, routine monitoring of vulnerabilities, and lifecycle maintenance of crucial software components.

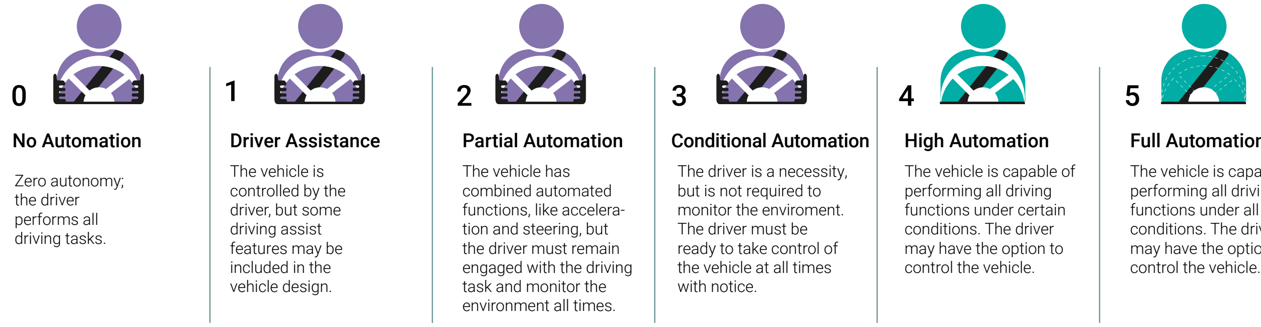
USD 56.67 billion

The size of the global autonomous vehicle market by 2026[5]

— Allied Market Research

> "94% of serious crashes are due to human error. 36,560 people died in motor-vehicle related crashes in the U.S. in 2018, highlighting the need for the lifesaving benefits of driver assistance technologies."[6]
>
> — United States Department of Transportation

With ADAS, there are five defined levels of assistance. As we move toward an era of fully automated vehicle operation, we are currently at level two as shown on Figure 2. Advances in artificial intelligence, particularly deep learning, will be necessary to complete the transition to fully automated operation. Safety considerations, protecting multiple systems against hacking attempts, and more sophisticated control systems will be needed to move forward in this area.



0 **No Automation**

Zero autonomy; the driver performs all driving tasks.

1 **Driver Assistance**

The vehicle is controlled by the driver, but some driving assist features may be included in the vehicle design.

2 **Partial Automation**

The vehicle has combined automated functions, like acceleration and steering, but the driver must remain engaged with the driving task and monitor the environment all times.

3 **Conditional Automation**

The driver is a necessity, but is not required to monitor the enviroment. The driver must be ready to take control of the vehicle at all times with notice.

4 **High Automation**

The vehicle is capable of performing all driving functions under certain conditions. The driver may have the option to control the vehicle.

5 **Full Automation**

The vehicle is capable of performing all driving functions under all conditions. The driver may have the option to control the vehicle.

Figure 2. Levels of automation on the path to fully autonomous vehicle operation[7]

[4] www.alliedmarketresearch.com/autonomous-vehicle-market

[5] www.alliedmarketresearch.com/autonomous-vehicle-market

[6] www.nhtsa.gov/technology-innovation/automated-vehicles-safety#topic-road-self-driving

[7] www.nhtsa.gov/technology-innovation/automated-vehicles-safety#topic-road-self-driving

Best Practices Underlying DevSecOps

As DevSecOps has been embraced by increasing numbers of organizations, a commonality of best practices has evolved.

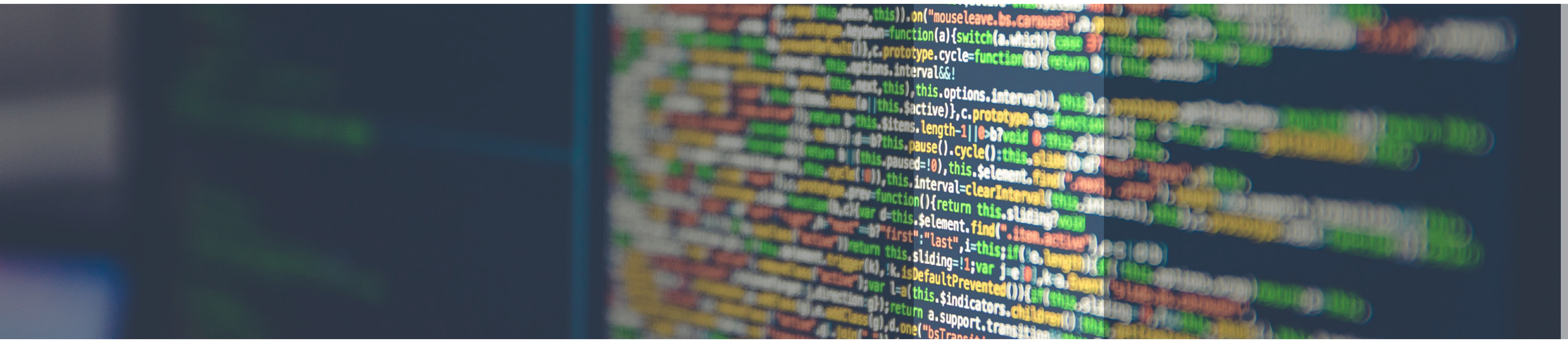
These provide an organizing framework for implementing software in which security is incorporated into the workflow. Recommended guidelines include these tenets:

1. Embed automated security controls and test sequences at the earliest stage of development.
2. Plan around the full software lifecycle to consider upgrades, patches, evolving vulnerability tests, and end-of-life provisions for the code.
3. Use tools that can scan code as it is developed to detect and resolve any security weaknesses.
4. Regularly check all code dependencies involving open source components to identify known vulnerabilities.
5. Apply static application security testing (SAST) tools to identify security flaws in both open-source code and compiled code.
6. Implement dynamic application security testing (DAST) sequences for simulating intrusions into the system.
7. Perform wide-scale threat modeling to locate vulnerabilities and mitigate any gaps in security controls.

This disciplined, thorough, and automated approach to security design and testing provides assurance that threat identification and elimination will be an integral part of a software solution. As shown in Figure 3, the pipeline encompasses all stages, from code selection and analysis through release and lifecycle management. For optimal results in maintaining 360-degree security during code updates, patches, and ongoing vulnerability testing, AI components are often used to manage update scheduling and deployment and perform frequent testing for detecting previously undiscovered threats. Software distribution through the cloud is becoming more common, with containers being used to safely and efficiently maintain a secure software environment within the vehicle.

The Role of Wind River in Advancing Automotive Technology

Solutions from Wind River have long been trusted components in demanding industries that require the highest level of reliability, security, and safety. This includes the building and maintenance of critical infrastructures, industrial manufacturing and machine processes, the aerospace industry, defense operations, and more. VxWorks® is a real-time operating system (RTOS) often selected for maximum reliability in mission-critical deployments, including high-profile space missions. Wind River has also excelled in the development and refinement of intelligent edge computing enhanced by 5G communications, enabling elaborate intelligent edge installations, which will be increasingly important in the future of autonomous vehicles and smart city transportation systems. Cloud technologies developed for delivering containerized software components to vehicles are another area in which Wind River has considerable expertise.



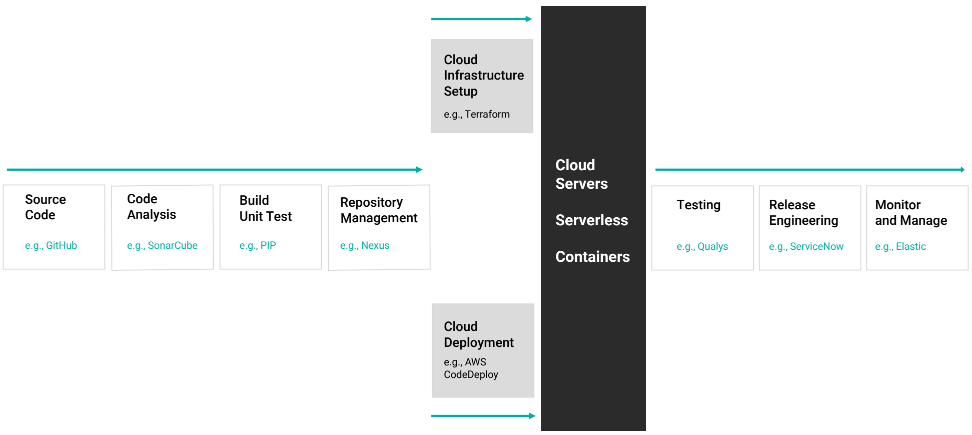


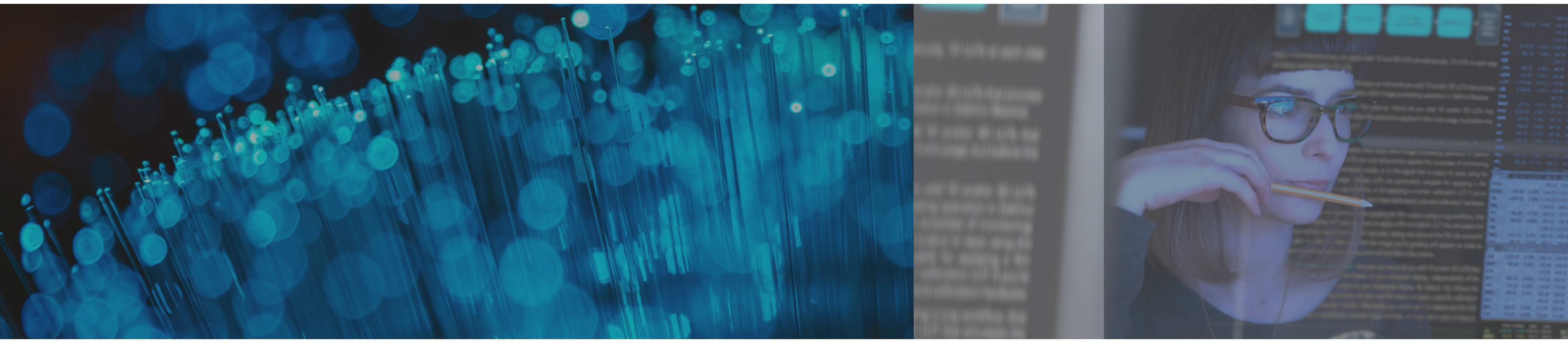
Figure 3. The DevSecOps pipeline emphasizes automated testing throughout the development cycle

In cases where there are multiple derivative products, to ensure software integrity DevSecOps tools can be used to automatically test the full range of possible cases for each. This is another area where AI can be employed to oversee the process and reduce potential errors due to faulty human decision-making.

With data for the vehicle and its operation being routinely collected and sent to the cloud, machine learning can be applied to continuously analyze possible safety issues in the software, perform predictive maintenance checks to warn the driver or servicing teams of pending component failures, or adapt the programming to be more efficient or to better respond to safety issues.

> "A typical new-generation vehicle likely has a software architecture composed of five or more domains, together comprising hundreds of functional components in the car and in the cloud. These cover everything from infotainment and ADAS to mapping, telematics, and third-party applications. Typical OEMs constructing this architecture interact with a multitude of software providers to build various capabilities; in the process they fill their vehicles with a broad set of development languages, operating systems, and software structures. This piecemeal approach is common among industry leaders because no single software platform on the market can meet all cross-system needs."[8]
>
> — **McKinsey & Company, January 2020**

[8] *www.mckinsey.com/industries/automotive-and-assembly/our-insights/the-case-for-an-end-to-end-automotive-software-platform*



SIMULATION TESTING IS AT THE HEART OF DEVSECOPS

To be effective in a DevSecOps model, consistent and frequent testing must be performed and repeated within a well-defined pipeline. Agile development can be effectively supported by a full-system simulator that models the functionality of hardware, operating systems, networks, peripherals, and boards. Wind River Simics® offers a powerful framework within which component operations can be precisely replicated, providing a test bed for designing and running new code, checking for vulnerabilities, developing fixes for problems that are detected, and assessing the overall integrity of the vehicle system. As shown in Figure 4, penetration testing is a necessity for keeping software components up to date and safe from intrusion as new hacking techniques are identified and their threats mitigated. Simulated penetration testing is designed to aggressively break through protections, finding ways to contend with existing, known threats without performing dangerous live testing of actual vehicles in traffic or on the open road. As indicated in the figure, this testing is part of a continuous cycle that goes through several stages and then is designed to start over again. This entire process can be automated and performed as frequently as needed to maintain the highest level of software integrity and security.

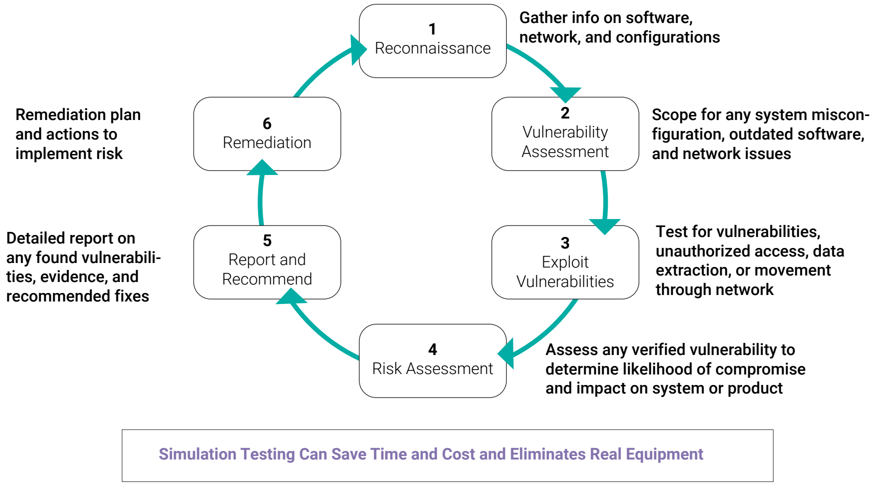

1
Reconnaissance
Gather info on software, network, and configurations
2
Vulnerability Assessment
Scope for any system misconfiguration, outdated software, and network issues
3
Exploit Vulnerabilities
Test for vulnerabilities, unauthorized access, data extraction, or movement through network
4
Risk Assessment
Assess any verified vulnerability to determine likelihood of compromise and impact on system or product
5
Report and Recommend
Detailed report on any found vulnerabilities, evidence, and recommended fixes
6
Remediation
Remediation plan and actions to implement risk
Simulation Testing Can Save Time and Cost and Eliminates Real Equipment

Figure 4. Penetration testing identifies weak points within a security framework

Wind River Solutions

Challenges presented by the increasing prevalence of software-defined vehicle operations are capably met by a portfolio of solutions from Wind River. VxWorks, Wind River Linux, Wind River Helix™ Virtualization Platform, and Simics have all been used in the automotive sector. Wind River Studio is a new integrated cloud platform that has been added to this portfolio. These solutions have been tempered and tuned in vast array of mission-critical deployments, including energy, aerospace, defense, medical, and manufacturing. When used in combination as part of platform solutions or infrastructure elements, these components can often save time in meeting certification requirements.

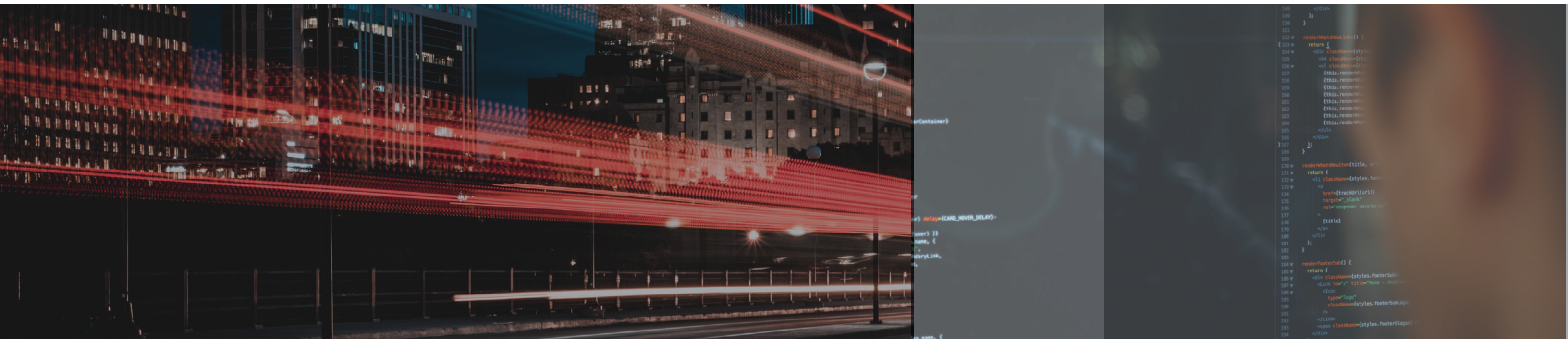
> "The Wind River Professional Services team brings decades of experience in hardening the security around embedded devices to protect them from cybersecurity threats."[9]

- **VxWorks:** The world's leading commercial real-time operating system (RTOS), VxWorks offers strong support for DevSecOps workflows for creating intelligent vehicle applications. During the development stage, VxWorks handles source code creation, code analysis, build and unit test, and repository management. VxWorks also supports Adaptive AUTomotive Open System ARchitecture (AUTOSAR), created by a development partnership of automotive entities establishing standards for automotive ECUs.

- **Wind River Linux:** Wind River Linux delivers commercial-grade functionality for embedded development and offers useful features for automotive applications, including rapid deployment of microservices and updates using container technology.

- **Wind River Studio:** Wind River Studio developer capabilities are integrated to deliver the only full-lifecycle management platform for intelligent systems at digital scale. Studio reengineers development workflows into solution sets that reduce development costs and accelerate capabilities for building, testing, and deploying on the edge.

[9] *blogs.windriver.com/wind_river_blog/2020/03/tools-for-agile-development*



- **Wind River Helix Virtualization Platform:** This software platform supports virtualized frameworks and offers a proven method for releasing code into production as part of a DevSecOps workflow. Helix Platform supports mixed-criticality OSes, providing the ability to run safety-critical and general-purpose applications side by side, while meeting the stringent requirements of ISO 26262 safety standards.

- **Wind River Simics:** By replicating the functionality of numerous kinds of hardware and operating systems, this full system simulator accelerates design, development, and testing of complex automotive systems while providing mechanisms to ensure safety and security. Simics accommodates agile and DevSecOps software practices and enables teams to shorten development cycles and thoroughly test embedded system designs without physical hardware present.

Future Directions

A convergence of several maturing technologies contributes to the advance of automotive safety and security, interoperating to enable vehicle-to-vehicle communication (V2V) as well as vehicle-to-everything (V2X) connectivity. Automotive solutions that incorporate DevSecOps practices typically rely on virtualization, cloud computing, elaborate simulations, a responsive RTOS, 5G communications, and a hardware platform that provides multi-core application support for redundancy, reliability, and performance. Wind River is committed to helping build a safe and secure future for the development and use of semiautonomous and autonomous vehicles, bringing together like-minded partners across a dynamic, worldwide ecosystem.

Wind River is a global leader of software for the intelligent edge. Its technology has been powering the safest, most secure devices since 1981 and is in billions of products. Wind River is accelerating the digital transformation of mission-critical intelligent systems that demand the highest levels of security, safety, and reliability.

© 2021 Wind River Systems, Inc. The Wind River logo is a trademark of Wind River Systems, Inc., and Wind River and VxWorks are registered trademarks of Wind River Systems, Inc. Rev. 02/2021