APTIV

CES 2026

Enabling the Intelligent Edge

KNOW BEFORE YOU GO

Redefining the Intelligent Edge

Walk into the Aptiv pavilion at CES 2026, and you'll immediately notice a difference this year. Next to the vehicles showcasing Aptiv's latest innovations in ADAS and user experience will be examples of our technologies in aerospace, telecommunications, industrial automation and robotics.

The vehicle is the most pervasive, most affordable and most interesting intelligent edge device in the world. It senses, thinks and acts in physical environments – and if you build it right, it can be continuously optimized to enhance each of those elements over its lifecycle.

We see other industries transforming, and their transformation looks a lot like what has been happening in automotive. Robots need software that doesn't fail. Cobots – collaborative robots – need sensing and perception systems that can identify objects and allow them to move safely among humans. Advanced air mobility solutions such as electric vertical take-off and landing (eVTOL) aircraft need software that supports mission-critical applications. Commercial vehicles need innovative cabin monitoring systems for long hauls. And companies need systems that connect this new world of the intelligent edge to the broader infrastructure that supports it.

Aptiv has a unique perspective. From software to sensors to connectors, we know how to build for both reliability and affordability – and we know how to deliver at scale. We bring that experience to diverse industries, but we also take the best practices from those other industries and use them to enhance our automotive technologies.

This backgrounder provides a sneak peek into what you can expect to see and hear from Aptiv at CES 2026 – in automotive and beyond.

Enabling the Intelligent Edge

We start with an overview of the edge-based AI that is transforming industries, with a thoughtful look at how this will play out by Javed Khan, Aptiv's executive vice president and president of Advanced Safety & User Experience. We examine the issue of trust in intelligent systems, and a specific case study of edge AI in action.

Intelligent edge systems get their data from sensors, and Aptiv made huge strides in sensing and perception this year. We have included in-depth Q&As on the latest generation of our radar technology and on the Aptiv PULSE™ Sensor, a unique combination of camera and radar in a compact form factor. And we discuss what the new technologies mean for ultrasonic sensors.

The heart of intelligent edge systems is in software, so it is vital to have the right software infrastructure platform, whether the edge system is a software-defined vehicle or something else. We've included our white paper detailing the platform components necessary. We discuss how cybersecurity will be more important than ever as threats evolve, and present another case study, this time highlighting user experience software.

In the next section, we explain how software development for the edge is different from development in the cloud and different from development for applications that are not mission-critical, with specific examples. Plus, we take a peek at a software challenge that could become more prominent in coming years.

We close with a look beyond the automotive industry. Our connectors are finding uses in other industries, our software is powering industrial automation, and we are trusted in satellites and space exploration.

We're excited to discuss these topics and more with you at CES 2026, as part of our ongoing collaboration to build the intelligent edge, in all its many forms.

Jeff Caruso
Vice President, Thought Leadership

Table of Contents

Edge AI

APTIV AT CES 2026

Living on the Edge: Where Physical and Digital Worlds Intertwine

The manifestation of artificial intelligence (AI) is undergoing a fundamental shift. Already, we're moving beyond the theoretical capabilities of AI in the cloud to explore its tangible impact on the physical world. Increasingly, the most transformative AI applications are emerging not just in centralized data centers, but also at the intelligent edge — the point where real-time sensing, decision making and action converge within integrated systems.

Consider the implications. From vehicles capable of navigating complex environments autonomously to industrial facilities that can dynamically adjust operations based on real-time data, edge-based AI is rapidly becoming the new benchmark for industries where speed, precision, safety and immediate responsiveness are critical.

This isn't a gradual technological evolution; it signifies a profound rethinking of where intelligence resides and how it can deliver tangible value on a massive scale.

The Intelligent Edge in Action

Currently, examples of edge-based AI include familiar applications like facial and fingerprint recognition on our mobile devices, or even more complex autonomous systems such as industrial robots or delivery drones.

While edge AI might sound abstract, its practical implementation resembles our own human body's intelligence system. Our body uses sophisticated sensors — our five senses — to capture environmental data: eyes detecting movement and light, skin sensing temperature, ears picking up sound vibrations and more. These sensory inputs connect to our brain — nature's powerful yet energy-efficient processing unit — which performs local computation without needing to consult external intelligence.

Our learned behaviors and reflexes function like lightweight AI models, optimized for instant on-device execution rather than requiring conscious thought. Underpinning these components is our autonomic nervous system — similar to specialized edge operating systems — designed for real-time processing of critical functions. Finally, our ability to learn from others and update our knowledge through communication mirrors the cloud orchestration aspect, enabling seamless connectivity and continuous updates across our distributed neural network.

This model is the functional blueprint that inspires advanced driver-assistance systems (ADAS) on the road today.

In a typical ADAS cycle, AI models function much like our human learning process. Just as we develop core skills through childhood experiences, these AI models are trained on extensive datasets before being deployed to the vehicle's sensory organs—radar and cameras that serve as the car's eyes and ears.

Our brain constantly processes new sensory information to refine our reactions and decision making. ADAS performs similarly by continuously gathering real-world driving data. This information flows back to update the core intelligence, similar to how our experiences shape our neural pathways. The improved understanding is then distributed throughout the fleet — comparable to how humans share knowledge through communication and learning from others' experiences. This creates a closed-loop system of continuous learning and enhancement that mirrors our own lifelong adaptation to new situations and environments.

As humans successfully adapt and transfer cognitive models across diverse situations — applying skills learned in one context to entirely different scenarios — the fundamental principles and technological components that enhance safety in vehicles can also be applied to diverse sectors such as healthcare, telecommunications, industrial manufacturing and robotics.

Truly, the underlying need for the rapid processing and localized intelligence unlocked by edge AI transcends specific industry applications.

Get a Head Start in Edge AI

For enterprises and organizations aiming to leverage the potential of AI at the intelligent edge, I've found that the following strategic steps can ensure a significant advantage:

- Identify key applications. Focus on scenarios where real-time insights and autonomous actions can yield substantial gains in efficiency, safety or customer/user experience. Consider applications in industrial automation, predictive maintenance or enhanced situational awareness in complex settings.

- Invest in infrastructure. This includes selecting edge hardware with adequate processing capabilities and energy efficiency, along with reliable sensor technologies tailored to the specific use case.

- Develop or upskill AI/ML expertise. Creating and deploying efficient AI models for edge devices requires specialized skills in areas such as model optimization and inference.

- Implement a management platform. This is key for scalability and maintainability. When vetting platforms, look for those that can deploy and upgrade AI models via over-the-air (OTA) updates, monitor device performance and ensure the security of edge deployments.

A well-defined orchestration strategy will facilitate the effective management of a growing number of intelligent edge devices and use cases.

The Real-Time Revolution at the Edge

The intelligent edge represents a significant evolution in how we interact with and utilize AI. It's not only about processing data closer to its origin; it's about enabling what can be described as "physical AI" —

intelligent systems capable of perceiving, reasoning and acting within the physical environment in real time. This interconnectedness is foundational to the next wave of innovation across numerous industries.

For example, in the context of modern vehicles, this entails more than radars that simply detect or recognize surroundings. It invokes a deeper, human-level of understanding, such as the ability to differentiate between similar objects in challenging conditions, to anticipate the behavior of pedestrians or adapt vehicle operation based on driver cues. These nuanced, context-aware decisions necessitate rapid processing and cannot rely on constant communication with a remote cloud.

Ultimately, the need for real-time intelligence at the edge is driven by the imperative for immediate and safety-critical actions.

While cloud computing will continue to be essential for AI development and data management, I believe the next significant advancements in AI-driven value will emerge at the edge. Looking ahead, the continued evolution and proliferation of the intelligent edge may democratize AI adoption across a wide spectrum of industries, inspiring innovative applications that we can only begin to imagine today.

Specifically, intelligent edge systems capable of sensing, deciding and acting in real time — in the real, physical world — are poised to unlock substantial improvements in efficiency, insights and safety. The foundational work being done to establish robust and scalable intelligent edge architectures in demanding environments is creating a transferable blueprint for broader transformation.

By embracing the intertwined principles of localized intelligence and real-time AI processing, organizations across diverse sectors can achieve smarter, safer and more insightful operations, paving the way for a truly intelligent, interconnected and more efficient enterprise.

This article originally appeared here.

Increasing Trust in Automated Driving

“Where’s my flying car?” drivers mutter as they wend their way through commuter traffic. “*The Jetsons* promised me a flying car by now.” Yet some of the same drivers have been hesitant to adopt nascent automated driving features available in today’s vehicles. OEMs are motivated to offer advanced driving features — with an emphasis on *advanced* — but adoption has been slower than many predicted.

What is holding drivers back from having enthusiasm for the technology? What can be done to encourage them to trust it? And how can OEMs benefit from the results? The answers, in short: Share information, demonstrate how well the technology meets expectations for a humanlike driving experience and encourage drivers to adopt the features gradually.

The autonomous driving features have to work

Plenty of us get into a car with someone whose driving acumen we distrust. Aunt Sandra imagines that she is a race car driver, cousin Ron has had a disconcerting number of fender benders, and buddy Todd persists in texting while behind the wheel. Nevertheless, we climb into the passenger seat.

But we expect more from automated driving systems. The automotive industry is working intensely to improve software-defined vehicles, including the AI and machine learning (ML) algorithms that enable them. OEMs are making ADAS more adaptive and developing better reasoning machines.

However, trust is about perception as much it is about objective reality. It takes time for new technologies to be accepted and then to become commonplace. In 1983, only 14 percent of drivers were using seat belts, despite plenty of research showing that the equipment saved lives. It took education, technological improvements and regulations to reach today’s 92 percent usage level.

It is one thing for automated driving to be safe; it also has to be perceived as safe.

To earn trust, an ADAS-equipped vehicle needs to deliver its promised user experience by making good, safe decisions while proactively and transparently communicating with occupants. Failures scare people away.

← TABLE OF CONTENTS

Offer gentle introductions

OEMs can help people learn what advanced driving features can accomplish by demonstrating them in low-stress situations.

For instance, automatic parking happens at a slow speed. If drivers do not like how the vehicle performs this maneuver, it is easy for them to cancel the operation and take over. At some point, after seeing the system's success, drivers may conclude that the auto-park feature is quicker and more accurate than they are. They are able to gain confidence gradually. That is how people learned to accept cruise control: They knew that they could resume manual control at any time with a tap on the brake pedal, and soon they learned that they did not need to.

One way to ease people on this journey is to moderate the output. Implementing an "explainer mode" in advanced driving systems can show a hesitant driver what the vehicle would do if full automation were turned on. The reasoning machine does its job, but it offers suggestions rather than taking over, much like a GPS that suggests an ideal driving route but does not compel a driver to follow it.

Another step is to tell the driver what the vehicle is doing. People may lack confidence that their ADAS will respond appropriately — *Will it stop in time?* — which puts them on edge. Vehicles can be designed to reassure drivers the same way humans reassure their passengers (like a parent saying, "Hang on, kids!" before making a hard turn or rapidly accelerating to pass another vehicle). With an explainer mode in place, the vehicle can say, "I see the bike on the side of the road. Don't worry; I'll stop if there's a problem."

With those guardrails, the driver eventually gains enough confidence to adopt ADAS suggestions. They can accept that the system is trained on actual human driving behavior from competent drivers and conclude, "I can enable the system on my commute, and I don't have to worry about it."

By offering people entry-level advanced driving capabilities, they can get used to such features before they explore more complicated options. This suggests market opportunities in scaling ADAS features from premium vehicles all the way to entry-level models. Doing so can democratize these features and help them gain broader adoption.

Use data transparency to share technology progress

ADAS features are advancing at an impressive rate, especially when it comes to safety. OEMs ensure that their vehicles comply with regulations and safety policies, though consumers notice such things only in their absence. They should tell people where the technology is — honestly and accurately — as well as where it is headed.

One virtue of AI/ML in automated driving is that these systems can learn. Data is collected and analyzed offline, using thousands of anonymized examples. Autonomous system efficacy thus improves over time, with later iterations making decisions that are safer, more efficient and so on.

OEMs should tell people when it does. Share hard numbers that make automated driving more compelling. Brag about technical improvements.

OEMs already collect and analyze a lot of data. They know how many miles people drive, how many of those miles are traveled using advanced driving features, the number of disengagements and in which scenarios the technology operates most efficiently. They can emphasize how much the automated driving features are tested — both in the real world and with synthetic miles — and back up that assertion with data.

← TABLE OF CONTENTS

OEMs can build on data-driven processes to improve confidence in autonomous transportation systems. We get into the car with Aunt Sandra despite her questionable driving skills because she has a driver's license (though it might have been renewed three eye exams ago). Appeal to that reliance on external assurance of safety by considering an industry effort to adopt principles of human-based licensing processes for certification.

Factual information reassures people. It helps them make better decisions, particularly when it is time to choose a new vehicle. Setting expectations accurately can convey how powerful and safe advanced driving systems are without suggesting that the technology is perfect.

An operational experience that combines ADAS features with user experience can create confidence among drivers, encourage adoption of these features and build trust over time.

Reducing Time-to-Market for Edge AI Applications

Wind River’s platforms are pre-integrated with Zededa and market-leading hardware to simplify the use of AI to improve industrial operations.

WIND RIVER AND ZEDEDA ENABLE INTELLIGENT SOLUTIONS

To improve safety and efficiency in industrial applications, Wind River® and Zededa have collaborated to deliver a pre-integrated solution for real-time, context-aware edge AI.

This approach powers critical applications — including computer vision, sensor analytics, industrial automation, and security — across a wide range of industries, such as manufacturing, healthcare, logistics, and energy. These kinds of applications require higher levels of safety, availability, and reliability than consumer applications.

By processing data locally at the edge, organizations benefit from lower latency, reduced bandwidth costs, enhanced privacy, and improved reliability, even in environments with limited connectivity. The solution from Wind River and Zededa enables developers to easily deploy such real-time, edge AI applications to address real-world problems.

Challenge

- Companies need systems that can make intelligent, real-time decisions
- AI solutions designed to make those decisions require support directly on devices where data is generated
- These mission-critical systems must be robust and reliable

Solution

- Created architecture to support AI-powered, context-aware applications, such as real-time detection of workplace safety violations
- Leveraged Zededa technologies for development, deployment, and management of edge AI applications
- Powered the solution with Wind River’s VxWorks® and eLxr

Results

- Lower latency and reduced bandwidth costs
- Enhanced privacy with all data processed locally
- Improved reliability

SAFETY AT THE EDGE

One important example of the need for edge AI is in the industrial market. Manufacturers form the backbone of modern economies, transforming raw materials and components into countless products globally. As intense competition, skilled labor shortages, inflation, and stringent quality expectations rise, manufacturers are increasingly turning to automation and more collaborative operation between humans and robots.

This is leading to new health and safety concerns, such as the risk of physical collision, the increased need for monitoring and oversight of often repetitive tasks, and the risk of system failures or unexpected behavior. Including traditional risks such as equipment malfunctions or human error, millions of workers are injured annually due to work-related incidents.

For businesses, the consequences can be severe, ranging from financial losses and operational disruptions to reputational damage, decreased workforce morale, higher turnover rates, and challenges in attracting talent.

A MORE INTELLIGENT APPROACH

In the ongoing race to address both efficiency and safety, new artificial intelligence (AI) tools offer immense promise. Executed well, they can transform industries by enabling real-time intelligence and decision-making directly on devices where data is generated, rather than relying solely on distant cloud servers.

However, edge AI is difficult to implement. This is particularly true for industrial applications, which must perform with a high level of safety, availability, and reliability, while remaining continuously certified and up to date.

Done right, edge AI can deliver powerful, scalable solutions that connect real-time data from complex, asset-heavy systems with digital enterprise processes, enabling smarter decisions, faster response times, and operational agility for companies across industries.

EXAMPLE: SAFETY CHECKS

The Wind River and Zededa solution is designed to prevent injuries by minimizing human error and enhancing workplace safety in environments with increased automation.

A camera monitors the manufacturing floor, and Zededa's advanced AI analyzes the image to ensure workers are equipped with the correct safety gear, such as hard hats and vests. When workers have the proper protective equipment, the system enables robots in the area to become operable. If someone removes a hard hat, for example, the system detects the change and instantly stops robots from operating.

Companies can deploy this kind of solution today with the following components from Zededa, Wind River, and our hardware partners. The following is a simplified representation of the solution stack used:

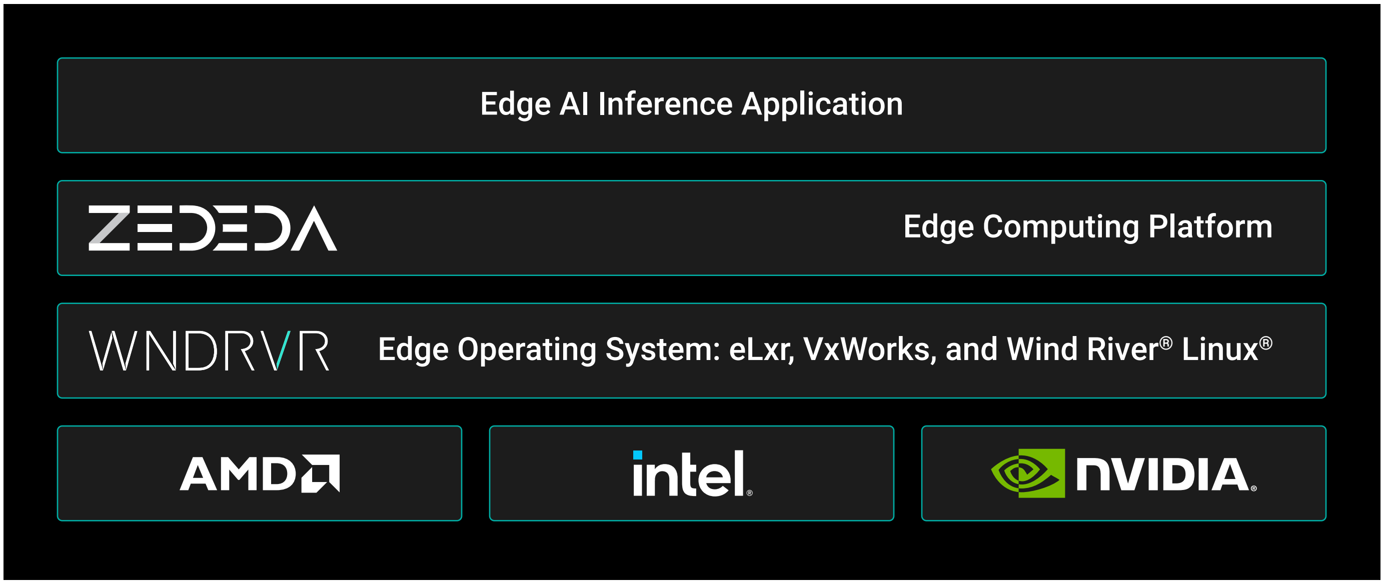
- Wind River's eLxr Pro™ and VxWorks for robotic arm control
- Zededa edge computing platform running as a virtual machine for edge orchestration
- AI-based inferencing application running in containers for object detection

ENABLING SOLUTIONS ACROSS END MARKETS

Edge AI promises to transform a wide range of industries.

INDUSTRY	EDGE AI SOLUTIONS
MANUFACTURING	Predictive maintenance, quality control, safety detection
ENERGY	Predictive maintenance, safety detection, flare detection
RETAIL	Stored intelligence, improved customer experience, shrinkage reduction
TRANSPORTATION	Predictive maintenance, physical security, safety monitoring
ROBOTICS	Safety detection, quality control, humanoid-robot training

← TABLE OF CONTENTS


Edge AI Inference Application
ZEDEDA
Edge Computing Platform
WNDRVR
Edge Operating System: eLxr, VxWorks, and Wind River® Linux®
AMD
intel
NVIDIA

Aptiv and Zededa have pre-integrated a solution architecture to flexibly support edge AI.

ELXR PRO

eLxr Pro from Wind River is a commercial enterprise Linux platform built for cloud-to-edge deployments. It offers long-term support, security monitoring, and customization services, making it ideal for critical workloads in industries such as autonomous vehicles, aerospace, energy, and industrial automation. eLxr Pro is optimized for containerized and AI workloads, supports remote updates, and ensures high performance and reliability. With expert backing from Wind River, it provides a secure, scalable, and open Linux solution for modern edge and enterprise server applications.

ZEDEDA EDGE COMPUTING PLATFORM

Zededa's edge computing platform addresses the challenges of distributed AI workloads, including scalability, diverse hardware, resource constraints, and intermittent connectivity. Its latest updates integrate NVIDIA's AI ecosystem — including the NGC Catalog, TAO Toolkit, and Jetson platforms — enabling seamless AI model development, optimization, and deployment at the edge. Organizations can pull models directly from NVIDIA's catalog, optimize them for edge use, deploy securely with zero-touch management, and monitor performance. Zededa empowers enterprises to accelerate AI initiatives, maintain infrastructure control, and scale from pilots to large deployments across complex edge environments.

Learn More

- Wind River Demonstrates Edge AI for Industrial Applications at Embedded World
- Zededa: How to Build and Deploy Scalable Edge AI with Zededa and NVIDIA
- Exploring the Future of Enterprise Edge AI: Zededa's Enhanced NVIDIA Integration
- Wind River: Enabling the New Industrial Age of Software-Centric Development and Operations

Intelligent Perception

APTIV AT CES 2026

Q&A: Key Technologies in Aptiv’s Gen 8 Radars

Aptiv’s latest radars boast significant technological advancements. The Gen 8 radars enhance performance, expand ADAS features, offer regulatory readiness and enhance cost efficiency —which sets them apart from previous generations and competing solutions. We sat down with Kyle Everly, Aptiv’s director of technical program management for radar perception, to find out more about the technologies that make Gen 8 one of the most compelling milestones in Aptiv’s quarter century of experience in automotive radar systems.

What are the key improvements in the Gen 8 radars?

Gen 8 radars combine proprietary hardware and software to deliver improvements in a number of areas. Two especially stand out.

First, we have upgraded RF [radio frequency] performance, which enhances range and coverage. For example, the FLR8 can support detection beyond 300 meters. The SRR8+ maintains Aptiv’s industry-leading range in the corner radar space, but it does that over a significantly larger vertical field of view compared with prior generations.

Second, we’ve improved horizontal- and vertical-angle performance by 25 percent over the previous generation. Both the FLR8 and SRR8+ are 4D radars, so they add the vertical dimension, which means they can separate object detection by vertical angle in addition to the horizontal angle. Importantly, they use a single transceiver. Such performance had previously been achievable only by cascading RFICs [radio-frequency integrated circuits], a design that is more expensive both in terms of power consumption and, ultimately, cost.

What do these improvements enable that couldn’t be done before?

Gen 8 radars will take current Gen 7 radar features and make them more robust and reliable, in addition to enabling them in more scenarios. They will unlock new ADAS capabilities as well. For example, we can offer automated parking beyond just controlled environments.

For features that already exist, such as determining the over- or under-drivability of objects in the road, the operational design domain is expanded, so features like automated emergency braking can be applied in more scenarios.

The high performance of the radars unlocks new possibilities in hands-free driving, which can now be performed in dense and complex environments, such as city streets and parking structures. The quality of the sensor data also improves features like scene perception and enables real-time drivable-space estimation.

We've doubled the number of channels. What does that mean for perception and, consequently, safety?

We've doubled the number of received channels, effectively doubling the amount of data available to perceive what is happening in the environment. That increase in data allows us to improve the speed and accuracy of object detection and classification, giving human drivers and ADAS more time to react in critical situations.

In terms of functional safety specifically, the radars will support an ASIL-B classification, including ASIL-B(D) in an ASIL-D system. Beyond that, Gen 8 radars will support future new car assessment programs and enable compliance with some of the upcoming regulatory requirements, such as FMVSS 127, by providing denser, richer and higher-quality perception data to the ADAS. With radar technology, we will achieve improvements regardless of lighting conditions, which means we can do that at night, in the dark, which is also an important test condition for FMVSS 127.

How do Gen 8 radars handle interference challenges, especially in dense and complex urban environments?

We've introduced new waveform techniques and countermeasures to better enable the separation of desired signals from interferer signals, which also helps with reflected signals. The custom processor in Gen 8 contains algorithms that not only detect and remove interference but also restore signals that have been corrupted by interference. This improved, restorative approach avoids signal-processing artifacts and maintains the dynamic range and detection capability, which improves the overall robustness of the radar in environments with many radars sharing the same frequency band.

How do Gen 8 radars handle detection of pedestrians and cyclists, especially in corner cases?

The 4D and fine-angle resolution of Gen 8 radars enhances object detection and classification, even for low signal-to-noise ratio [SNR] targets and in environments that require high dynamic range. This improvement enables the detection, separation and tracking of targets that were missed in prior generations of radar, allowing for better detection of vulnerable road users, especially in challenging scenarios, such as a pedestrian standing next to a parked car or another highly reflective object.

Could you explain dynamic range and its effect on resolution?

Dynamic range refers to the full span of changing conditions. If we have better dynamic range, we're able to detect a small target in the presence of a large target. "Small" and "large" here don't necessarily mean physical size; they mean reflectivity or signal-to-noise ratio. For example, while a driver can see that a pedestrian is standing near a truck, with radar the pedestrian may be "masked" by the truck or, in essence, lost in the shadow. Without excellent dynamic range, the radar can't pick the pedestrian out of the data.

One of the cases where this comes into play is if you have two targets at the same range and moving with the same speed, but one is low SNR and the other high SNR. In those situations, which often occur in urban and parking scenarios, previous radars would struggle to pick up the low-SNR target. Improved dynamic range helps us to identify both of those targets, which expands the availability of features, including pedestrian AEB [automatic emergency braking] and automated parking.

A significant part of the value that we bring is in the signal processing of that data and knowing how to extract the most out of a given antenna.

GABOR VINCI
Head of Business Development, Active Safety

Q&A: Aptiv PULSE Sensor – A New Take on Perception

OEMs continuously balance sensor cost, vehicle safety and streamlined installation. To meet those requirements, Aptiv created the Aptiv PULSE (Parking, Urban, Localization and Surround Enhancement) Sensor, an innovative sensing device that integrates a surround-view camera with an ultra-short-range radar in a compact, ice-cube-size package. In this Q&A, Gabor Vinci, Ph.D., Aptiv's head of business development for Active Safety and "the father of PULSE," discusses this new perception sensor that provides a cost-effective way to achieve more precise parking and low-speed maneuvering, as well as heightened highway awareness.

What is the Aptiv PULSE Sensor?

PULSE is a surround-view camera and a miniaturized radar integrated into the same housing. It can be packaged in the same installation positions as a surround-view camera. The important difference is that in addition to having an optical path that gives you an image, it allows you to perceive the environment with radar, so you have two sensing modalities in one compact housing in the same location in the vehicle. There's no need to search for additional packaging spaces in the vehicle.

What makes PULSE valuable for OEMs?

PULSE can help OEMs create a better, more reliable system that is also cost optimized. We estimate that PULSE will help to reduce the overall cost at the vehicle system level by nearly 15 percent.

You can use the same single physical connection that already exists for the camera so the wiring is shared. The video stream and radar data are serialized into a single link and sent to a central compute unit — a central vehicle controller or domain controller, for example — which then deserializes and processes the two streams. This layout allows the customer to reduce complexity and cost by reducing the wiring and the number of sensors while also being able to increase perception quality and reliability.

Can PULSE be used in entry-level vehicle models, where we don't typically see surround-sensing systems, or is it only for premium vehicles?

It can be used for both premium and entry-level systems. Rear-facing cameras are mandatory for the largest markets around the globe. You need to have a visual device, plus a cable, installed in every single car that you sell. But you can place PULSE and get rid of all the ultrasonic sensors in the back of the vehicle.

For the front, if there isn't already a parking camera, you could introduce PULSE to give the driver a front visual aid as an additional feature. This adds the cost of processing and transmitting a video stream, and it isn't mandated, but it gives an OEM the option to offer additional value for the customer. It is up to the OEM to decide whether they want to offer a value-add for the brand and accept additional data cost in the vehicle.

Having said that, I would call it a nice feature for the final customer. You have multiple options because you do not need 100 percent, 360-degree sensing. It's something that should be discussed platform by platform, depending on the OEM's scaling strategy.

Can PULSE be integrated with an existing system?

Yes, but there are prerequisites. There must be a deserializer that is compatible with the serialization protocol of the device. There also has to be enough compute and memory allocated on the compute device to perform the post-processing required by PULSE. If those prerequisites are there, then there is no issue in integrating PULSE into an ECU [electronic control unit] that has been created by someone else.

If Aptiv delivers the compute unit we can guarantee compatibility, and that the software is allocated with enough memory and adequate throughput.

What use cases would PULSE support? How many sensors would you need for those scenarios?

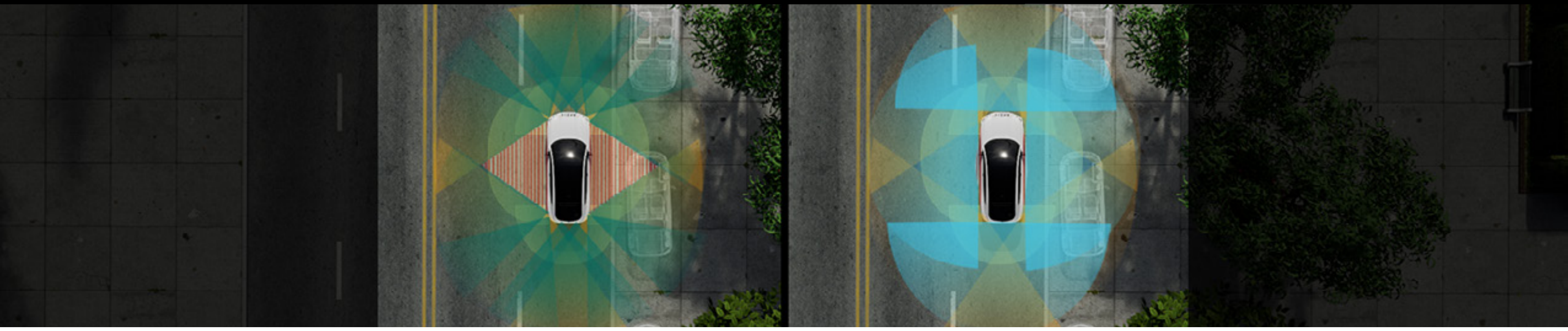
It depends on what you want to do. For example, if you want to get rid of the current parking systems and enhance the capabilities, you need one sensor in the back and one sensor in the front, and then you can get rid of a 12-channel ultrasonic system. This would allow you to maneuver safely and reliably in a complex environment.

It is very rare for a car to have sensors on the sides, which means there is no real-time tracking of any object that comes close to the doors of a vehicle. Typically, the tracking systems remember what the sensors have seen before and extrapolate that movement. In contrast, if you include PULSE on the side of the vehicle, you could have that capability, completing the 360-degree coverage. Even in poor-visibility conditions, you'd be able to sense obstacles right next to the car. That would be the ultimate real-time solution that allows you to create safer features for maneuvering in urban environments.

It also allows you to create more safety features for driving. Say, for example, that you are in a dense traffic jam and there's a motorbike driving close to you. The bike might be in your blind spot. PULSE could reliably detect that area and help you avoid an accident.

Will PULSE be a single product for global usage, or will there be different flavors for various regions?

It's a sensor system that is envisioned to work in the upper ultrawide frequency band, between 76 GHz and 81 GHz, so it can be operated in Europe and North America. The main mode of operation will be 76 GHz to 79 GHz, which provides excellent resolution and also allows the system to be operated in China as well as Korea. Japan is coming soon. We've got the largest markets in the world covered.



Going a Step Beyond Ultrasonic Sensors

Ultrasonic sensors specialize in short-range detections of obstacles and are widely used in automotive applications to help ADAS perceive the world around a vehicle. But while they are useful, ultrasonic sensors also have limitations that could be addressed by emerging sensing technologies.

When it comes to mobility, ultrasonic sensors put the “bat” in Batmobile — they use the same echolocation technique as bats to navigate. Both send out high-frequency soundwaves that reflect off of objects to establish location and proximity. In this way, the sensors have helped drivers avoid bumping into nearby vehicles and other close obstacles for decades.

Colloquially called “buttons,” ultrasonic sensors are known at a glance by automotive designers. They may be overlooked by consumers, however, because they appear as relatively small dots color-matched to the bumpers and other body panels they are mounted within. A typical vehicle may have as many as 12 ultrasonic sensors installed to cover its perimeter.

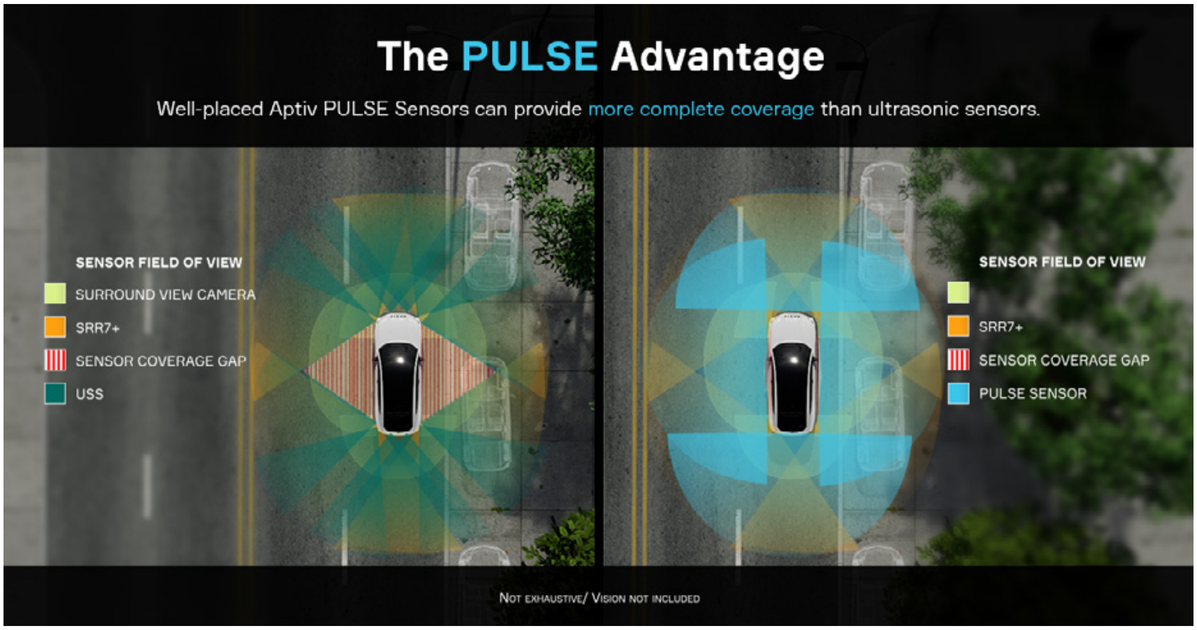
Multiple sensors are required because a single ultrasonic sensor cannot resolve the angular position of an object on its own. To get a more accurate picture of the environment, an ultrasonic-based perception system must incorporate a constellation of sensors, using an algorithm to interpolate between their signals. While the resulting reconstruction of the vehicle’s surroundings may be adequate for some automated parking scenarios, the range of conditions under which it will work — its — may be limited, and the speed of completion of a parking maneuver may be slower than desired.

In addition, ultrasonic sensors do not work well on vehicles moving at speeds above 35 mph. Because they use sound waves for detection, they are limited by the time of flight of those sound waves moving through the air, which is, of course, much slower than electromagnetic waves travel. They also have a lower refresh rate than is needed at higher speeds, lack doppler optimization (the ability to detect frequency shifts) and can suffer from signal interference in inclement weather. Finally — and unsurprisingly for a technology that relies on sound waves — loud noises in the vehicle’s vicinity, such as a jackhammer in use, can sometimes result in false detections.

While those limitations do not affect the low-speed functions that drivers rely on, such as parking-distance warnings, they leave an opening for a technology capable of higher precision and less vulnerable to interference.

Radar and cameras have both served to fill those gaps. Radar is far less subject to signal interference and environmental conditions, such as fog, and cameras offer detailed, full-color images, allowing accurate obstacle classification. The ideal solution is sensor fusion, which combines each type of sensor's strengths. Using multiple sensing modalities has typically required separate hardware and wiring, which increases cost, weight and complexity.

Aptiv met this challenge by introducing the Aptiv PULSE™ Sensor, an innovative perception sensor that combines a camera and an ultrashort-range radar into a compact one-box, one-wire solution.



In a recent Q&A, Gabor Vinci, Aptiv's head of business development for Active Safety and "the father of PULSE," explained what makes PULSE so novel: "PULSE is a surround-view camera and a miniaturized radar integrated into the same housing. The important difference is that in addition to having an optical path that gives you an image, it allows you to perceive the environment with radar, so you have two sensing modalities in the same location in the vehicle." This configuration provides overlapping strengths while reducing the amount of wiring needed. This results in lower costs and, importantly, lower latency, which can boost reaction time by critical milliseconds.

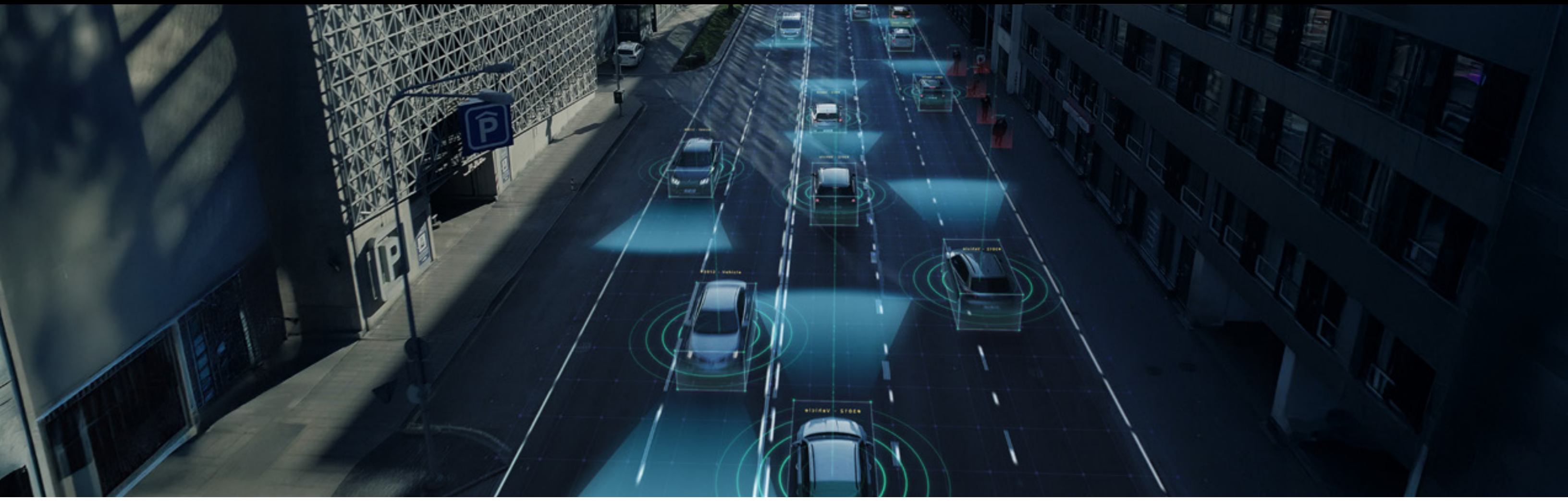
PULSE can match the short-range capabilities of ultrasonic sensors, but the radar component has better long-range capabilities, which — especially when combined with the camera component — can be used to usher in advanced driving functionality.

These innovations allow PULSE to help fulfill the dream of fully automated parking and give it the ability to safely navigate through dense urban environments, without its effectiveness being diminished by bad weather or other interference.

Despite their limitations, however, ultrasonics remain valuable for drivers. There are many situations where Batmobiles and other vehicles can still take advantage of well-established ultrasonic technology for the critical task of obstacle avoidance. With ultrasonic sensors, radars, cameras and now PULSE, OEMs have a range of choices when developing future models.

Software & Services

APTIV AT CES 2026



A Cross-Domain Software Infrastructure Platform Is Necessary for Cloud-Native SDVs

As vehicles evolve into software-defined systems on wheels, consumers are demanding more personalized experiences from those vehicles. That means the software needs to do more: It has to act as an intelligent edge device, uniting functions and data not just from various domains within the vehicle but also from the cloud.

Whether the functions reside in a different application or operating system or in a cloud-based data center thousands of miles away, they all have to be easily and seamlessly linked together and remain responsive without experiencing life-threatening latency.

The solution is a comprehensive software infrastructure platform that is modular, hardware-agnostic and cross-domain, allowing it to be flexible, future-resilient, safe and secure. It must provide an open software framework with a developer-friendly environment that embeds edge analytics, containers and over-the-air (OTA) update capabilities for continuous and sustainable lifecycle management.

This approach is both more cost-effective and more adaptable than current alternatives and will lead the automotive industry and other mission-critical industries into the software-defined future.

A SOFTWARE PLATFORM FOR A NEW WORLD

Vehicle software applications used to be confined to individual domains, such as infotainment, ADAS, powertrain and body control. Each acted independently in individual electronic control units (ECUs) that were often dedicated to a single function and could not be updated easily.

Today, the world of vehicle software is much broader. Cloud connectivity can enable OTA updates, offload compute-intensive tasks and aggregate data from multiple sources, including other vehicles, to deliver advanced services and analytics. These capabilities improve performance and reduce hardware costs, but they also introduce significant challenges in coordinating real-time operations without latency risks.

What is needed is a unified, cross-domain and cloud-native software platform to enable consistent communication, dynamic updates, remote diagnostics and efficient lifecycle management — a platform that unites fragmented systems to achieve better scalability and decrease development complexity and cost. This platform must balance workloads across systems, enable seamless communication between services, optimize resource use, reduce complexity and accelerate innovation across the vehicle.

The traditional approach is to connect operating systems and applications through middleware, a layer of software that standardizes the interfaces between them and acts as a translator to ensure that applications can communicate effectively with various hardware systems without needing to be tailored to each specific component.

LIMITATIONS OF MOST MIDDLEWARE

With middleware, a developer can write a software application once and know that it can run on various hardware and operating systems without needing to be rewritten to fit each one. Middleware takes care of the details, letting OEMs focus on developing the business value in software-defined vehicle (SDV) applications, from personalized infotainment offerings to critical updates.

But middleware is just one piece of a much larger puzzle. And despite the many advantages middleware offers — such as abstraction, interoperability and scalability — today's market dynamics have exposed significant limitations. Originally designed with high expectations and adopted widely across industries, many traditional middleware solutions have become increasingly complex and rigid, frustrating developers and slowing innovation.

A common pain point is API fragmentation. Application programming interfaces are the point of contact between applications and the functionality that middleware provides. As the functionality evolves, it can be difficult to maintain compatibility between APIs and applications. As a result, many platforms fail to address the real-world challenges of modern software architectures and lifecycle management, such as compatibility among disparate offerings, hampering optimal performance and restricting the ability to perform timely upgrades. Done right, middleware should not merely comply with specifications — it should actively remove barriers to efficient development, deployment and evolution.

While interoperability is the core promise of middleware, most current offerings fall short by locking developers into proprietary ecosystems. From the middleware itself to associated tools and training, organizations often find themselves dependent on a single vendor. This vendor lock-in leads to inflated costs, limited flexibility and constrained innovation. Customizations can incur exorbitant fees, so development teams are forced to adapt their workflows to rigid vendor-prescribed models — often requiring steep learning curves and productivity trade-offs.

These challenges are not confined to a single domain within automotive. Whether it is ADAS, infotainment, powertrain control or body electronics, the need for open, modular and developer-friendly middleware is increasingly critical. Each of these domains faces unique integration and lifecycle hurdles, yet they all benefit from platforms that enable seamless interoperability, reduce vendor lock-in and accelerate development. There is a clear opportunity for middleware solutions that go beyond compliance — empowering OEMs and suppliers to innovate across domains without being constrained by proprietary ecosystems or rigid workflows.

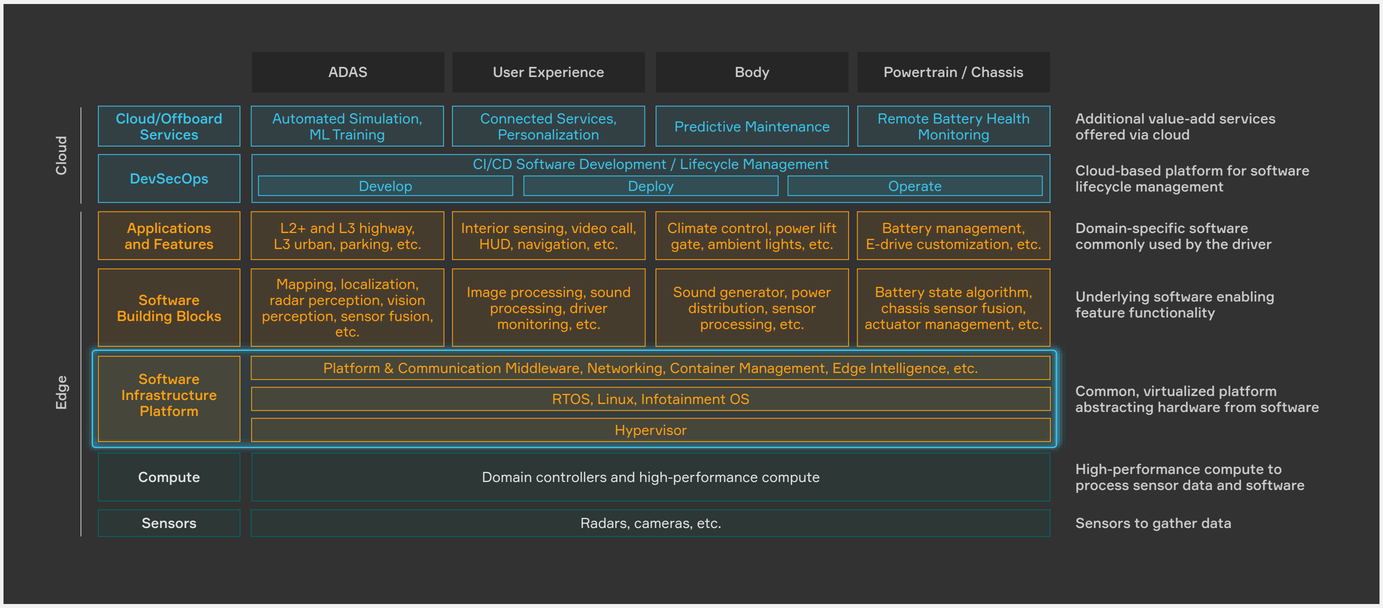
KEY ELEMENTS OF SOFTWARE INFRASTRUCTURE PLATFORMS

Even with middleware that meets these requirements, more is needed to fully support SDVs. A software infrastructure platform must have several key elements. The well-orchestrated interplay among them is essential to achieving a safe, flexible and cost-effective development environment for SDVs. Among the top requirements are:

Over-the-air updates. OTA is a key enabler of the software-defined vehicle, allowing for real-time updates and design flexibility. Secure and reliable OTA updates allow OEMs to deploy new features, bug fixes and security patches to vehicles already on the road, keeping fleets current and competitive. OTA updates enable consumers to avoid dealership visits, increasing customer satisfaction. For OEMs, OTA updates save money by not requiring manual labor from a service technician. OTA warranty fixes can achieve near-complete coverage in a matter of days. When paired with vehicle diagnostic tools and processes, automotive OTA updates can reduce warranty costs by up to 50 percent for addressable software-related items.

CLOUD-NATIVE SDV ARCHITECTURE

Speeds development, streamlines deployment and optimizes lifecycle



		ADAS	User Experience	Body	Powertrain / Chassis	
Cloud	Cloud/Offboard Services	Automated Simulation, ML Training	Connected Services, Personalization	Predictive Maintenance	Remote Battery Health Monitoring	Additional value-add services offered via cloud
	DevSecOps	CI/CD Software Development / Lifecycle Management Develop Deploy Operate				Cloud-based platform for software lifecycle management
Edge	Applications and Features	L2+ and L3 highway, L3 urban, parking, etc.	Interior sensing, video call, HUD, navigation, etc.	Climate control, power lift gate, ambient lights, etc.	Battery management, E-drive customization, etc.	Domain-specific software commonly used by the driver
	Software Building Blocks	Mapping, localization, radar perception, vision perception, sensor fusion, etc.	Image processing, sound processing, driver monitoring, etc.	Sound generator, power distribution, sensor processing, etc.	Battery state algorithm, chassis sensor fusion, actuator management, etc.	Underlying software enabling feature functionality
	Software Infrastructure Platform	Platform & Communication Middleware, Networking, Container Management, Edge Intelligence, etc. RTOS, Linux, Infotainment OS Hypervisor				Common, virtualized platform abstracting hardware from software
	Compute	Domain controllers and high-performance compute				High-performance compute to process sensor data and software
	Sensors	Radars, cameras, etc.				Sensors to gather data

Fig. 1. A cloud-native software infrastructure platform for SDVs enables faster development, better security and lower costs.

DevOps. A software infrastructure platform must support industry standards and the full software lifecycle, from development and testing to deployment and operations, allowing developers more flexibility and customization so they can innovate faster, reduce costs and maintain software quality across vehicle generations. Most importantly, the platform must respect developers' own workflows and not impose external frameworks that can cause delays and unnecessarily complicate internal processes.

Containerization. Cloud environments depend on containers to isolate applications and manage their deployment. With the help of an in-vehicle container orchestrator, applications can be deployed, updated and tested independently of one another, making the software development lifecycle far more agile. For example, developers can create test environments for new features, simulate those features' behavior in real time and deploy updates over the air without disrupting other vehicle subsystems. This container-based approach ensures faster integration and testing because it corrals potential issues and reduces the complexity of testing different systems together.

Microservices and security. Secure containerized environments foster trust among OEMs, Tier 1 suppliers, and software partners, enabling safe codevelopment and integration across the SDV ecosystem. Containerized microservices ensure secure and resilient software deployments — protecting vehicle systems and user data while complying with automotive cybersecurity regulations, such as UNECE WP.29 and ISO/SAE 21434. In a properly configured software infrastructure platform, each containerized microservice is isolated, reducing the effects of attempted attacks. Security policies can be applied at the service level, enabling granular control and minimizing systemic vulnerabilities. This ensures that only verified, trusted containers are deployed in production environments.

Network management. SDVs need to manage a growing array of interconnected domains. A software infrastructure platform should allow for the seamless management of network configurations, enabling the proper handling of security protocols as well as real-time communication between multiple modules, subnetworks and applications, thus reducing latency to enhance critical safety and functionality in the vehicle.

Edge intelligence. A well-developed software infrastructure platform should allow for seamless and customizable data collection, enabling OEMs to easily collect and manage various types of vehicle data — including controller area network (CAN), Ethernet, media, diagnostic, network and ECU statistics — without requiring separate, dedicated hardware or customized agents running on each ECU. Real-time data collection provides OEMs with insights into system performance and driver behavior, supporting continuous improvement in vehicle quality, safety, customer experience, cost optimization and fleet management. By understanding how systems and drivers interact, OEMs can refine features and personalize experiences — making the driving experience safer, smoother and more intuitive.

Determinism. It is essential that a software infrastructure platform perform in a deterministic manner — even across individual components — because ISO 26262 compliance requires deterministic execution of safety-critical tasks. In an SDV, operations such as braking and lane-keeping must be performed within strict timing constraints and without unpredictable delays. Deterministic behavior ensures that sensor inputs, actuator commands and control loops are processed in real time, which is critical for maintaining vehicle responsiveness and operational safety. Deterministic systems are easier to test, validate and debug. Engineers can reliably reproduce issues, which is essential for regression testing, certification and long-term maintainability.

The abstraction of middleware. When part of a larger software infrastructure platform, middleware provides more value than when used in traditional approaches. It holds the other elements together, allowing them to be drawn upon as necessary. Middleware abstracts the underlying hardware and communication protocols, allowing software components to be developed, tested and updated independently of specific hardware configurations. This abstraction enables seamless portability across different systems-on-a-chip (SoCs) and device classes and facilitates cross-domain data exchange, ensuring interoperability across heterogenous systems and ECUs. There are three different levels of abstraction that middleware must provide:

- **Communications.** Middleware abstracts communication protocols by elegantly hiding the complexity of underlying transport layers (such as CAN, Ethernet and SOME/IP) while allowing developers to focus on application logic instead of low-level communication details. This facilitation of cross-domain data exchange ensures interoperability across heterogenous systems and ECUs.

- **Operating systems.** Modern vehicles can contain more than 100 ECUs, each running its own OS. Middleware allows developers to smoothly work within this complexity by standardizing communication protocols between ECUs, managing cross-domain functionality and providing data pipelines for edge AI applications, ensuring consistent access to sensor and actuator data regardless of the OS.

- **Hardware.** The right middleware allows for greater flexibility in hardware design, permitting an SDV to be hardware-agnostic. Developers can select whatever SoCs are appropriate, and middleware will help applications run on them. In addition, middleware allows projects to be ported without excessive updating. Applications developed for one type of vehicle can be reused in other types, without developers having to rewrite the code.

A software infrastructure platform helps designers move from building software for isolated ECUs to integrating them as a unified system. It helps with vehicle lifecycle management, such as overseeing how data is being obtained from vehicles. In turn, that data informs decisions about which components and functions need to be updated and when, in a digital feedback loop.

THE FUTURE

OEMs that are serious about building and maintaining a competitive advantage must go beyond exploration to natively build software-defined vehicles. In this market reality, OEMs should seek a vendor that can provide a comprehensive software infrastructure platform that incorporates advanced middleware techniques to enable efficient lifecycle management for generations of software-first vehicles. This approach will reduce costs and production time while increasing opportunities for customization and domain-specific architectures both at the edge and in the cloud.

A software infrastructure platform can also extend beyond automotive to power intelligent robotics systems, from autonomous drones to mobile robots. As AI-based autonomy scales across industries, OEMs will require a modular, secure and real-time infrastructure to build, deploy and evolve intelligent machines at the edge.

In an increasingly AI-driven industry, where vehicles are intelligent edge devices that interact with the cloud, and OEMs must reckon with the complexities of physical AI across multiple domains, OEMs will need a trusted, experienced partner that can provide an end-to-end software solution with support services to ensure a smooth workflow, solid architecture and reliable performance for their customers.

Aptiv is that partner, providing a comprehensive set of software and tools through the Aptiv Layered Infrastructure for Networking and Compute™ (LINC™) Software Platform. With LINC, OEMs are well positioned for a software-defined future.

ABOUT THE AUTHORS

Craig Turner
Vice President and Managing Director, Digital Cockpit and Middleware

Craig Turner leads Aptiv's infotainment, interior sensing, and software infrastructure platform product lines, creating next-generation in-vehicle experiences. Since joining Aptiv in 2020, he has driven customer engineering for user experience products, delivered engineering services, and established Aptiv's DevSecOps practice. With more than 23 years of experience in software and embedded systems across automotive, mobile, robotics and gaming, Craig is a passionate advocate for software-driven transformation.

Niheer Patel
Head of Product Management, Middleware & DevOps

Niheer Patel oversees Aptiv's software infrastructure platform, driving software-defined transformation through scalable middleware and DevOps. With 20 years of experience in embedded software, safety and security, he has led the development and certification of mission-critical software infrastructure for the automotive, aviation and industrial markets, shaping the future of intelligent mobility through innovative products.

LEARN MORE AT APTIV.COM/MIDDLEWARE →

Why It’s Time to Invest in Quantum Cybersecurity

Until now, computing has been based on binary numbers: ones and zeros, true or false, on or off. In contrast, quantum computing supports multiple states, exploring trillions of possibilities all at once — which makes it sound like something out of science fiction.

But quantum computing has stepped out of the realm of science fiction and into reality. Striving to outpace major competitors like IBM and Google, Microsoft announced the development of a palm-sized quantum computing chip earlier this year. Computer scientists can already see how quantum computing may make the world better, where it may be able to solve problems a million times faster than today’s computers, and where technical advances could decrease the physical size of quantum computers.

Breakthrough work is genuinely underway. Viable paths for scaling quantum computers to millions of qubits are now clear.

But while quantum computing promises to deliver more computational power, it also brings new dangers. Encryption systems that protect data today will become vulnerable when practical quantum computers arrive in seven to 10 years. Quantum computers capable of breaking current cryptographic standards represent a threat to the privacy of individuals and the security of organizations and entire nations.

This is a ‘today’ problem

While seven to 10 years may sound like a long way off, preparation for quantum threats must begin now, not once they have already materialized. Organizations need time to implement post-quantum cryptography (PQC) transition plans methodically — and that applies both to anyone with an IT infrastructure and to anyone building software-defined systems.

“Current encryption, such as RSA and ECC [elliptic curve cryptography], will become obsolete once quantum computing matures,” said Cigent cofounder John Benkert. “Management often assumes cybersecurity threats are only present-day problems. But this is a future-proofing issue — especially relevant for industries dealing with sensitive, long-lifespan data, like healthcare, finance or government.”

Remediation requires long-term planning. Organizations that wait until quantum computers have broken encryption to address the threat will find that it is too late.

One reason for the urgency of starting today is that an adversary could harvest data now and decrypt it later, once large-scale quantum computers become available. The threat of "capture now, exploit later" means that quantum-resistant algorithms must be deployed well in advance of the scaled quantum computers required to fully execute such an attack.

The good news: Much of the groundwork has been laid. In 2024, after seven years of international collaboration, the U.S. National Institute of Standards and Technology (NIST) finalized its principal set of post-quantum cryptographic algorithms. However, those algorithms have to be added into common and not-so-common protocols, including Transport Layer Security (TLS), which underlies web browsers.

"Every security protocol that uses public-key encryption and digital signatures now needs to be updated to use the new post-quantum standards. So TLS has to be updated to use post-quantum encryption, and the digital certificates TLS uses to authenticate endpoints have to be updated to use post-quantum signatures. In fact, every use of public-key digital signatures needs to be updated," explained Brian LaMacchia, a cryptography engineer who oversaw Microsoft's post-quantum transition from 2015 to 2022 and has since founded Farcaster Consulting Group.

And that is just the beginning of the process. Making those updates will entail a lot of work for security professionals, and weaving those changes throughout existing systems' infrastructures will take time. Fortunately, adding quantum resistance to new systems does not add more time to development schedules, and it does not cost more. The algorithms are free. PQC processes do not require more expensive chips, though they might use different ones. It's a matter of using newer and different chips and algorithms, not necessarily more expensive components.

As with Y2K so many years ago, quantum's biggest challenges are around existing systems. Each company needs to identify and update all of its large software stacks and convert their existing uses of cryptography to the new algorithms. But implementing PQC will be more challenging than addressing the Y2K problem was, LaMacchia contended. The problem is harder to describe, and remediation is more difficult. Without tuning or upgrading systems, replacing cybersecurity algorithms can affect application and network performance.

And, critically, with Y2K, everyone knew what the deadline was. With quantum cybersecurity, the deadline is fuzzier. Would-be adversaries do not issue an announcement when they acquire new abilities to breach systems.

What quantum cybersecurity means to mission-critical industries

In some industries, product lifecycles are fast. However, industries that build equipment intended to operate for decades — such as automobiles, aircraft and oil pipelines — need to design secure systems that can withstand breach attempts for years to come, not just today.

To do that, firmware updates need to be digitally signed by the manufacturer, and those digital signature algorithms need to be quantum resistant to ensure that a vehicle does not load a malicious update, LaMacchia said, warning, "If somebody breaks your digital signature, they can impersonate you."

Automotive OEM encryption systems use cryptography to check manufacturers' digital signatures, such as when validating firmware updates and application code in software-enabled vehicles. Broken authentication lets bad things happen. Someone could remotely take over a vehicle, for instance, or send malicious code for autonomous execution later, even after the vehicle has gone offline.

However, the new quantum computing cybersecurity algorithms are larger than the old algorithms. "The key sizes are larger, and the ciphertexts are larger, which means you need more storage space," LaMacchia said. Relative to the size of most systems, the additional space is small, but in tight, embedded systems, "the code needs to reflect those changes," he added.

What to do about it today

Here are a few steps companies can take today to prepare for potential quantum security threats.

Build an inventory. Identify what needs to change across toolchains. Itemize everything used today, as well as who owns its implementation and the process of updating it.

"Who owns the physical devices that are securing your VPNs?" LaMacchia asked. "Who owns the storage encryption? For the encryption you're using, is that something you do in software? Is it the hardware manufacturer?" Don't leave anything out, he advised.

With inventory in hand, LaMacchia said, go down the list and say, "OK, how am I going to update this for PQC?"

Avoid adding technical debt. Start using quantum-resistant cryptography today, and begin building crypto-agility into the lowest layers of the system.

That is not a new concept for engineering teams. Cryptographic security already comprises a montage of different algorithms. Engineers can augment traditional asymmetric cryptography algorithms with the algorithms from the new NIST standard.

Make the technical adjustments. The new PQC algorithms are larger and more complicated than the ones engineering teams are used to. In some cases, digitally signed messages with security information could triple in size, which could impact storage and bandwidth.

For example, LaMacchia said, someone building oil pipelines might want to install low-power sensors every kilometer, with batteries that will last five years. Tripling the amount of energy required for compute and wireless low-power messages could decrease battery life. Without careful integration of the new algorithms, systems will not last as long as their specifications require.

Ensure that suppliers are quantum-ready. All of the suppliers in an OEM supply chain need to be on the same page. Requests for proposals should ask vendors to include a PQC update plan. Will they automatically update the product or service? What assurances do they offer? Getting answers to such questions is particularly critical for any proprietary protocols, such as those used in many manufacturing systems.

How are we helping?

Aptiv thrives within the tight constraints of the embedded edge, incorporating artificial intelligence into edge devices such as jets, vehicles and robotics and helping to ensure that they are quantum-ready. We are working closely with semiconductor companies, and we demonstrated chip-accelerated quantum resistant cryptography at the Consumer Electronics Show in 2025. To learn more, ask your Aptiv representative about quantum-ready product security.

Developing Zeekr's Infotainment System Required Tight Teamwork on Tight Deadlines

OEMs need a partner that is not just reliable but also deeply knowledgeable, flexible and quick to respond. Premium Chinese electric vehicle brand Zeekr chose Aptiv to be that partner as it sought to enhance its user experience offerings by incorporating Qualcomm's latest Snapdragon SA8295, a new system-on-chip (SoC) specifically designed for automotive infotainment.

As a testament to the competitiveness and speed of the local market, Zeekr set an aggressive deadline of only 14 months from start of development to start of production (SOP). It sought a technical partner to provide a stable platform that would include hardware and base software to run and integrate the applications and human-machine interface it was developing.

Zeekr aimed for two SOPs, with uncompromising targets. The initial production launch would be October 2023, with a second set for March 2024. To meet their deadlines, Aptiv's team members challenged themselves to develop two different hardware platforms simultaneously rather than following the usual sequence of completely developing one and then using it as the framework for the next. This way, they could rapidly and efficiently lay the foundation for four vehicle models.

Collaboration at the Forefront

Aptiv's digital signal processor (DSP) experience is one example of what made it an ideal partner to help Zeekr achieve its tight deadlines on budget. It recognized that incorporating an audio DSP into an infotainment system SoC could save the OEM from having to integrate a separate XMOS chip for audio, and thus reduce the overall system cost. OEMs have historically not made full use of the DSP cores on their main SoCs, but Aptiv, with its decades-long expertise in DSPs, was able to integrate an audio DSP into the SoC, streamlining the system and saving bill-of-materials costs for Zeekr.

The scope of work also included combining the driver cluster and in-vehicle infotainment system into one box. That required significant computing power, including CPUs and GPUs, as well as NPUs (neural processing units) — chips purpose-built to run AI and machine learning algorithms.

Aptiv provided the majority of the software, incorporating QNX as the base operating system and creating middleware, drivers, audio and DSPs. The mandate from Zeekr included implementing brightness functions in FOTA (firmware over-the-air) technology and getting the microcontroller unit and SoC to communicate, as well as optimizing bandwidth utilization and reducing transmission errors. To fulfill these highly resource-intensive requirements and meet the tight timelines, Aptiv dedicated its own local engineering talent, drawing from a pool with deep expertise in software tools.

Navigating Twists in the Road

When a memory chip shortage affected the original design, the difficulty level went up another notch, requiring a major change three months before the second deadline. The team essentially had to skip what would have been a 2.0 release and went directly to a 2.5 release. The challenge played to one of Aptiv's strengths: handling logistics and supply change management on a tight turnaround.

Aptiv's long-established connections with Chinese vendors and manufacturers mean that it is well positioned to support such mitigations to facilitate operations at scale. Aptiv has made supply chain resiliency a hallmark of how it supports customers, including creating a digital twin that traces supply chain sourcing, fluctuations and potential disruptions in real time.

Supporting the revised scope also required revalidating safety-certified systems, retooling, and performing other critical revamps in manufacturing — all challenges that Aptiv has extensive expertise in handling. Much of the eventual success was due to the seamless coordination between the Zeekr and Aptiv engineers, who worked as one team to deliver the project while coordinating closely with Qualcomm to expedite deliveries.

Lessons Learned

Success comes from a culture of partnership and flexibility matched with the engineering expertise to quickly execute on inevitable challenges and necessary changes in scope. Aptiv succeeded because its engineers could draw from decades of experience in DSPs; advanced compute, validation and testing; integration of software applications from a wide range of sources; and sophisticated supply chain management that includes digitized, unified tools and deep local vendor relationships.

Challenge

- Develop an infotainment system using a novel chip and integrate the customer's intellectual property
- Meet an aggressive deadline of only 14 months from start of development to SOP
- Revamp the original product in three months to meet a new scope of work

Solution

- Apply supply chain expertise, along with integration, test and validation expertise, to meet sourcing requirements for a new deadline
- Draw on DSP expertise to deliver cost-effective and creative results
- Collaborate as a trusted technology partner with the customer and industry suppliers

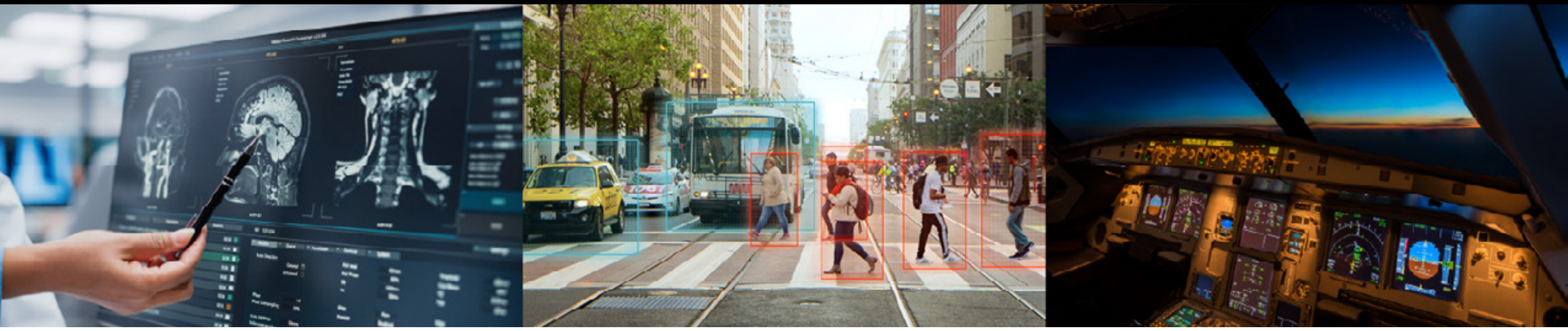
Results

- Product met both original and accelerated deadlines
- Costs met customer expectations despite a revamped scope

← TABLE OF CONTENTS

Developing for the Intelligent Edge

APTIV AT CES 2026



Developing Innovative Software Without Breaking the System

For years, universities and the corporate world have channeled students into one of two general groupings. One set is taught skills that they use to build amazing consumer technology, much of which manifests as apps that live on smartphones. The other group of developers is equipped to create business-to-business (B2B) commercial applications, most of which reside in the cloud.

Unfortunately, the lessons learned by both consumer and B2B developers do not translate well to the world of mission-critical applications. In these systems, such as ADAS, medical and surgical equipment, and telecom satellites, failure truly is not an option.

Consider the Silicon Valley mantra of “move fast and break things.” The reasonable premise is that development teams should iterate, try new things, learn from mistakes and improve with every iteration.

> “Move fast and break things. Unless you are breaking stuff, you are not moving fast enough.
>
> - Mark Zuckerberg
>
> *CEO, Facebook*

Agile development practices add well-tested functionality gradually. But "move fast and break things" suggests that it is worthwhile to make mistakes and disrupt technologies in the name of innovation rather than play it safe by working at a slow and steady pace. The motto has taught a whole generation of software developers to value speed over stability. It suggests that change, as opposed to creating stable systems built for the long term, is always a good thing. And entire ecosystems feed into this approach.

Consider also Jeff Bezo's API Manifesto. Twenty years ago, Bezos mandated that all of Amazon's internal systems must expose their data and functionality through APIs. That approach was essential to the establishment and success of Amazon Web Services — but it also taught a new set of developers to build things in the cloud with the expectation of nearly unlimited resources.

Now combine those two trends. The vast majority of developers begin their careers expecting no restrictions or limitations on the way they code. They believe that they have the entire cloud to power their applications and the tacit permission to move fast and break things.

Those premises work well for consumer mobile apps and B2B information technology efforts, but they are anathema to anyone who builds systems that can never fail.

The Difference With Mission-Critical Applications

Every project has hardware constraints and budget limitations. But mission-critical software has additional needs — and those needs often conflict with the two approaches mentioned above.

Most cloud B2B applications and consumer software can be updated regularly. It is less feasible to push fixes to edge computing devices that operate at low bandwidth or with limited storage. Designing for hardware such as medical devices, portable point-of-sale devices and remote sensors requires developers to consider factors such as storage space, weight, power consumption and duty cycles. Such devices certainly lack the unlimited power of the cloud or the certainty of guaranteed connectivity.

The projects for these complex systems often have extended time frames. They can take years to design and launch properly. The original hardware may be several generations old by the launch date, so the systems must be designed to adapt over time to avoid becoming outdated.

Mission-critical systems often require safety testing and other certifications to ensure that the application continues to function flawlessly in worst-case scenarios. Any changes or updates, however minor, may require recertification.

Iterative development certainly can work in these environments. However, in this context, "moving fast" occurs at vastly different speeds. A consumer app that measures a diabetic's glucose level can be updated daily, if necessary. That is not so for the patient-monitoring equipment used during surgery. And the seemingly infinite cloud storage that developers take for granted is rarely an option for devices that must function even when connectivity is lost.

AI Complicates Things

Mission-critical systems must behave consistently and predictably. An application should always produce the same output when given the same input and starting conditions.

Mission-critical applications must be aware of changes introduced by over-the-air (OTA) updates. Updating the software alters the original profile, rendering the safety evidence irrelevant. That has been a challenge for as long as OTA updates have been around, but experienced embedded systems developers have adjusted their processes accordingly.

AI, by its nature, is not deterministic — and it will be increasingly less deterministic.

Need a hands-on example? Ask ChatGPT a question. Then, two days from now, ask it the exact same question. See if the answer changes. Sometimes it does; sometimes it does not. But by default, large language models are not set to react in a deterministic way because of the variables, the stimuli and the range of different permutations that affect it. So the AI built into mission-critical applications must be able to shift as well.

That makes development — and the regulations and certifications designed to provide assurance of their performance — more difficult.

Building Toward a Third Path

The development approaches of moving fast and taking advantage of unlimited cloud scale are not wrong or broken. They are exactly what were needed to drive the innovation we have seen in certain industries. But as intelligence shifts to the edge and we see machines becoming smarter and more autonomous, there will be an increasing need for a third approach to systems development, where reliability and stability are the key mantras. The organizations that can innovate in those environments will become the next set of market leaders.

What Makes ‘Mission Critical’ Different?

By Sandeep Modhvadia, Chief Product Officer, Wind River

Wind River has served the embedded systems community since the introduction of VxWorks in 1987. We understand the diverse range of possible software applications for embedded systems and edge computing, wherein hardware is also an essential element. Our unique perspective, gleaned from the experiences of countless unique customers and applications, offers several examples to illustrate the distinction between mission-critical computing and consumer or business-to-business (B2B) computing.

Don’t be distracted by the overused term. Every application is “mission critical” to the people who rely on it. A time-tracking application failure might be a crisis for a marketing agency, and a connectivity dropout could play havoc with a retail point-of-sale system. However, while such failures may be emotionally upsetting and financially distressing, lives are typically not at risk.

The requirement “This application cannot fail” may suggest that quality assurance and security testing are all that is needed to prevent a failure from occurring. However, with mission-critical applications, every unique requirement impacts the application infrastructure and the decisions made throughout the development lifecycle. The following real-world examples from Wind River customers illuminate the challenges of, and the technical remedies for, the development of mission-critical systems.

AEROSPACE: THE SOFTWARE THAT CONTROLS JET AIRCRAFT CANNOT FAIL

If you have traveled on any commercial jet in the past 20 years, it almost certainly ran Wind River software.

Developers and engineers design cockpit controllers and other aerospace components for worst-case scenarios. One way to ensure that everything continues to function correctly is to incorporate isolation into their systems. That is, one system can run completely independently of another, even when being executed on the same silicon. A technical element in this effort is to enforce robust partitioning through a hypervisor or complete hardware isolation.

MEDICAL SYSTEMS: A VENTILATOR CANNOT BE REBOOTED IF A PATIENT IS ATTACHED TO IT

One ventilator manufacturer had a patient on its life-support equipment for three years. The ventilator never failed, and it was never restarted. A reboot could not be allowed to happen: If the equipment had been turned off, the patient would have died.

Consider the system architecture challenges in ensuring that a device will operate continuously -- no restarting or refreshing. They encompass everything from managing resources efficiently to ensuring a constant steady state despite an ongoing stream of data that has to be managed. How do you perform a critical update or fix a security vulnerability? Mission-critical systems have those requirements as table stakes.

THE SPACE CASE: "WAIT UNTIL IT'S PARKED OVERNIGHT" DOES NOT APPLY TO A MARS ROVER

VxWorks provides the core operating system of the Mars rover Curiosity. NASA can remotely send software updates to the spacecraft using an updating mechanism, not dissimilar to how vehicles receive over-the-air (OTA) updates.

The mission-critical element here is how such updates work. Nobody would perform an update on a vehicle while it was driving down a street. Most updates happen overnight, when vehicles are parked. If an OTA update fails for any reason, the system — the vehicle — can be reverted back to a stable version at the dealer or with the help of a mobile service technician. But if NASA encountered the same issue, it could "brick" Curiosity — without anyone available to reboot the system.

The rover may be an extreme example. However, many other edge systems are equally inaccessible (in the practical sense, anyway) and therefore require the same level of forethought and validation regarding system updates.

AUTOMOTIVE APPLICATIONS: ASSISTED DRIVING SYSTEMS MUST PERCEIVE EMERGENCIES AND RESPOND TO THEM WITH PRECISION

Imagine a car equipped with self-driving features at a four-way stop. As the vehicle proceeds through the intersection, an 18-wheeler suddenly appears that will be unable to stop. Can the advanced driving system react fast enough to recognize the approaching truck and then either apply the brakes or the accelerator to avoid an accident? Can it speed up even if it means overriding the digital controls to exceed the acceleration guidelines?

In scenarios like this, microsecond precision and responsiveness matter. The system certainly cannot get stuck in an undefined state where it is unclear what it should do.

Nor is this challenge unique to automobiles. Many devices require split-second analysis based on inference at the edge, along with near-instant response times and the ability to respond to external stimuli. These automotive mission-critical lessons apply to many other industries.

TELECOM: CALLS CANNOT BE DROPPED, EVEN IN A CRISIS

The 2025 Eaton fire in Southern California destroyed more than 9,000 structures. During the crisis, a major telecommunications company — a Wind River customer — had to ensure that 911 emergency calls in the area were never dropped. When someone calls emergency services, they need adequate time to articulate their location and describe the problem. A dropped call could mean the difference between life and death.

Given that level of urgency, any cellular network operator must invest in reliable emergency services with optimal throughput — and do so affordably. The company concluded that it needed to isolate its hardware from software. That led to larger architectural decisions, such as the best way to create abstraction layers and the degree to which the company could deploy off-the-shelf hardware.

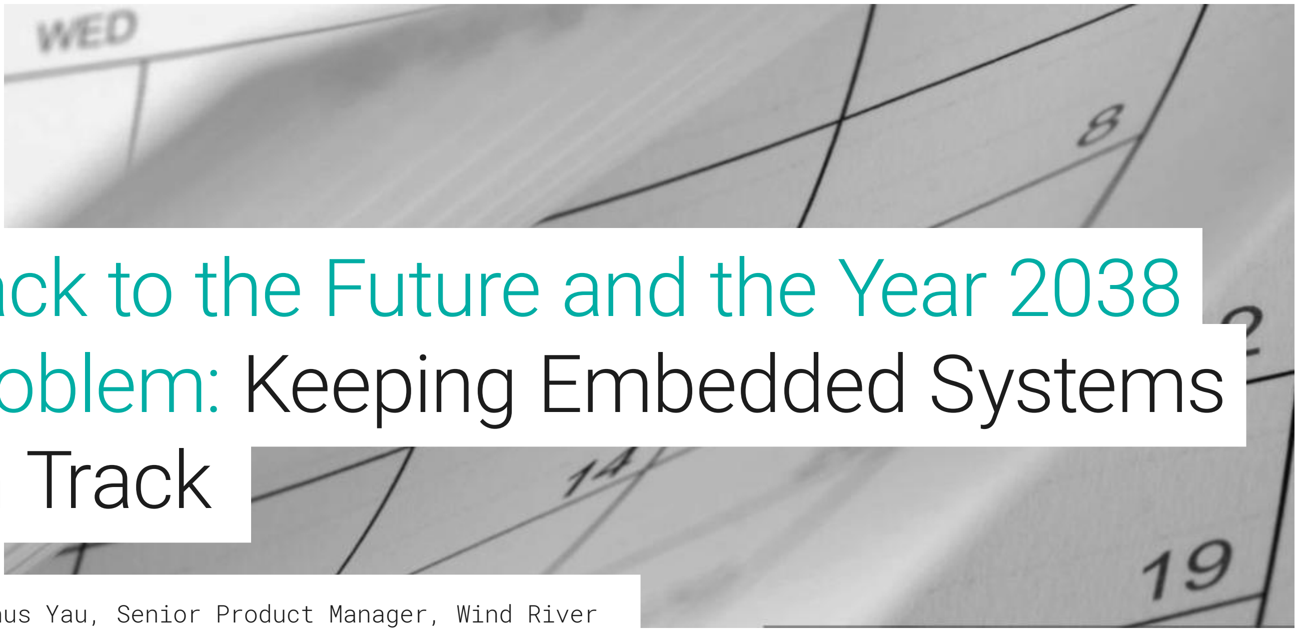
A MINDSET SWITCH

Those examples are merely a sample of the circumstances that turn an application development project into a mission-critical endeavor. Those requirements usually add time to a project. The application must work reliably for years on equipment that would otherwise be replaced, and it must be capable of (certifiable) upgrades that provide the same assurance of quality as earlier versions.

Because it is difficult or impossible to apply a "move fast and break things" approach to developing mission-critical applications, the design process often takes longer than consumer or B2B developers expect. For instance, they have to make difficult hardware choices (since the lifecycles of these expensive systems can be measured in decades) and plan for exhaustive compliance testing.

The good news is that information is being shared across industries, making it easier to design, deploy and maintain mission-critical applications. Supporting our customers connects us with engineers who design and deploy mission-critical (and sometimes not-so-critical) embedded systems, leading to many interesting conversations. Aptiv and Wind River play an active part in organized information-sharing activities, such as sponsoring the recent IEEE Space Computing conference and actively participating in open-source projects such as OpenInfra and Linux distributions.

← TABLE OF CONTENTS



Back to the Future and the Year 2038 Problem: Keeping Embedded Systems on Track

By Janus Yau, Senior Product Manager, Wind River

If the Back to the Future movie franchise taught us anything, it's that time travel can be thrilling. But in the embedded world, unexpected time jumps are anything but fun.

Imagine this: It's January 19, 2038. A satellite that's been running flawlessly since 2023 suddenly believes it's 1901. Logs go haywire, systems misfire, and engineers are left scratching their heads. What happened?

Welcome to the Year 2038 problem: a real-world time glitch that could affect long-lived embedded systems. Fortunately, VxWorks® has already taken the DeLorean out for a spin and made sure your systems won't get stuck in the past.

WHAT IS THE YEAR 2038 PROBLEM?

Many embedded systems use a 32-bit signed integer to represent time as the number of seconds since January 1, 1970 (the Unix epoch). This format maxes out at 2,147,483,647 seconds, which lands us on January 19, 2038, at 03:14:07 UTC.

After that? The counter flips to a negative number, and systems start thinking it's 1901. That's not just confusing — it can lead to data corruption, system crashes, or unpredictable behavior.

The problem probably sounds familiar. In the early days of computing, software developers took similar date storage shortcuts (for example, using 89 to represent the year 1989), which led to the Year 2000 problem. Fortunately, by working together, the computer industry identified Y2K vulnerabilities and addressed them well in advance. As a result, few computers worldwide malfunctioned on January 1, 2000. It was handled so well that some people today trivialize the significant technological and industry achievement.

It's time to repeat the exercise for the Year 2038 problem.

WHY EMBEDDED SYSTEMS ARE ESPECIALLY VULNERABLE

Embedded devices are built to last. They run for decades without updates, they power critical infrastructure (such as satellites, industrial robots, and medical devices), and they use real-time operating systems (RTOS) with strict timing requirements.

These systems can't afford to get the date wrong. And they definitely can't afford to misbehave.

VXWORKS: YOUR SHIELD AGAINST TIME-TRAVEL GLITCHES

Wind River saw this challenge coming and acted early.

VxWorks 7 has supported 64-bit time stamps since 2020, which means it has:

- 64-bit time_t support across kernel and user space
- Updated API support for both 64-bit and legacy 32-bit systems
- No date overflow in 2038, plus seamless support for dates far into the future

If you're building new systems today, VxWorks 7 is your go-to platform for long-term reliability.

Still running VxWorks 6.x? You're not alone. That's why Wind River released RCPL8 for VxWorks 6.9.4.12 in 2025, adding Year 2038 support for key components and migration guidance to help you transition safely.

The Year 2038 problem is real — but it's also manageable. If you're building or maintaining embedded systems, here's your checklist:

1. **Audit your code:** Are you using 32-bit time_t?
2. **Check your OS version:** Are you on VxWorks 7 or a patched 6.x?
3. **Plan for the future:** Especially for systems with long lifespans.
4. **Talk to Wind River:** We have the tools and expertise to help.

With VxWorks, you're not just avoiding a glitch. You're building systems that last, perform, and won't blink when the clock strikes 2038.

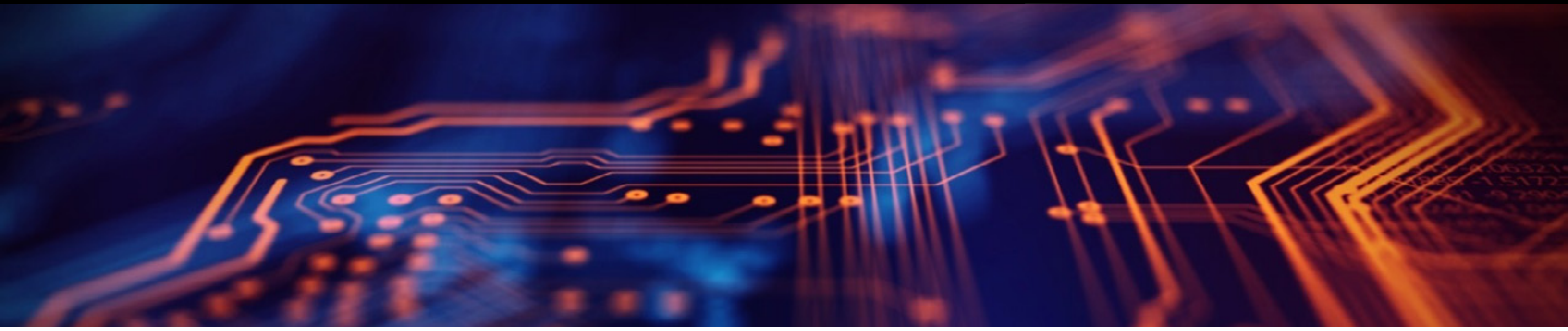
Time flies — but with VxWorks, your systems won't lose track.

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.

← TABLE OF CONTENTS

Cross-Industry Innovation

APTIV AT CES 2026



Automotive Connectors: Not Just for Automotive Anymore

Satellite components and automotive components might seem like two disparate types of technologies, and indeed, for a long time, they were nearly as far apart as Detroit and Mars. But as more satellites are launched — more than a dozen a day now, on average — the satellite industry is looking for the same fundamental qualities that have worked so well in automotive: durability, reliability, scale and cost-effectiveness.

Good technology often finds unexpected uses far beyond what was originally intended. The transistor was invented not to create a digital revolution but merely as a more efficient alternative to fickle and cumbersome vacuum tubes. While transistors first found an obvious home in telecommunications, engineers in other sectors quickly realized that if you had a switch that was extremely reliable and could be miniaturized, even the sky was not the limit.

Similarly, there is opportunity for superior technologies to cross over in the area of connection systems. All electrical devices, from robots to automobiles to satellites, face an important design question: how to consistently deliver power and data throughout their machinery, however challenging the operating conditions may be.

A history of innovating in multiple ways

The crucial requisite for connectors, dating back to the earliest days of electrical wiring, is a contradiction: a component that will not shake loose but can be decoupled for maintenance. The ideal connector is designed with “secondary assurance,” a double-locking system that ensures a mated pair stays tight. This need must be satisfied at scale.

The automotive industry met that requirement long ago, with connectors for vehicles ranging from passenger cars used for stop-and-go daily commutes to heavy farm and construction equipment that must function in the full spectrum of environmental conditions. The best proof of such connectors’ reliability is their decades of success in a broad range of use cases.

Over time, along with enhancements in form and materials to increase resistance to corrosion, vibration and thermal stress, connectors gained digital intelligence. They became part of increasingly complex automotive electronics systems that now run on the Controller Area Network bus standard or, in the most recent iterations, single-pair Ethernet, which makes them even more analogous to other advanced systems.

For automotive OEMs, a connector is a commodity component, made by the millions and priced accordingly. Connectors specifically designed for use in other industries serve similar functions, but because demand for them has been more limited, manufacturers have not been able to take full advantage of economies of scale. Nor do those bespoke connectors have a track record of millions of miles of reliable use like automotive connectors do.

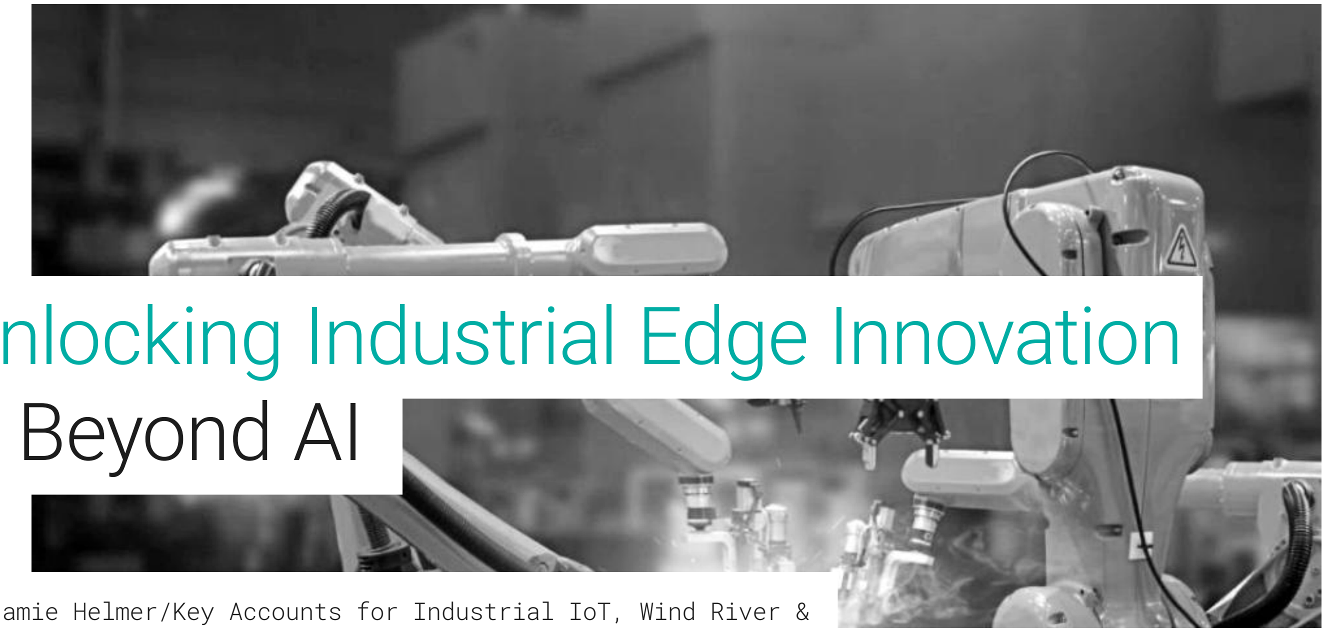
Innovations that other industries can tap into

The ability to provide robustness at consumer price points has attracted the attention of other industries looking for connectors for tailored purposes without bespoke prices. For example, the automotive industry's early adoption of single-pair Ethernet has increased the appeal of automotive connectors in other sectors.

Additionally, automotive protocols have extended into new markets. USCAR (United States Council for Automotive Research) standards — originally developed for automotive manufacturing — are increasingly being adopted in other industries, particularly in industrial automation and robotics, due to their emphasis on interoperability, data communication and smart manufacturing.

But there are considerations that must be taken into account in transitioning between industries. For example, because the automotive industry is primarily consumer-directed, and cost optimization has been at the forefront, design engineers have eschewed exotic materials for lower-cost ones that can be easily sourced. Other industries, especially aerospace, may need materials with higher heat tolerances than automotive. As a result, additional testing and validation of automotive connectors may be required in such industries.

Nevertheless, connectors with automotive roots will remain a compelling choice that will increasingly show up in industries far from their point of origin. They could even be used in the data centers that power AI. If that happens, the technology will have come full circle, as software-defined vehicles pull data from cloud platforms hosted in data centers that are using automotive connectors.



Unlocking Industrial Edge Innovation – Beyond AI

By Jamie Helmer/Key Accounts for Industrial IoT, Wind River &
Lexi Schroeder/Sr. Product Line Manager, Wind River

AI leads the headlines. But industrial automation success requires attention to other technologies and business practices.

Industrial environments are notoriously diverse. They combine legacy industrial control systems (ICS), programmable logic controllers (PLCs), and supervisory control and data acquisition (SCADA) systems with modern IoT sensors, cloud-based services, and AI/ML workloads. This mix creates an intricate landscape that must operate cohesively under constraints that include limited bandwidth, intermittent connectivity, and resource scarcity.

AI might be part of the solution, but to tame the complexity and unlock innovation, industrial organizations need a cohesive strategy that includes the right security, the right technologies, and the right people with the right training.

STRENGTHENING SECURITY IN DISTRIBUTED EDGE ENVIRONMENTS

As computation moves closer to where data is generated — on factory floors, oil rigs, or wind turbines — new security challenges emerge. Traditional IT security practices can fall short because they were designed for centralized, high-bandwidth environments. They struggle to account for the distributed, offline, and physically exposed nature of edge deployments, and they aren't adaptable or granular enough to secure diverse edge nodes operating in harsh or remote conditions with limited oversight.

Many organizations are responding with a defense-in-depth approach:

- Zero-trust architectures: These include secure boot, trusted platform modules, and hardware roots of trust to ensure device integrity. They treat every connection as untrusted by default, ensuring least-privilege access across the environment.
- Immutable infrastructure and signed updates: Infrastructure cannot be changed once deployed, which reduces drift and tampering risks.
- End-to-end encryption: This is instituted to safeguard sensitive information — for example, TLS for data in transit and LUKS for data at rest.
- Identity and access management (IAM): These are among the practices that ensure that only explicitly permitted people and systems can perform an action on a particular resource. They bring robust authentication and access controls to remote nodes.

MANAGING RISK AND COMPLIANCE AT SCALE

In large-scale industrial ecosystems, it can be daunting to manage risk and compliance across thousands of edge devices. For example, each device may run a different software version, collect sensitive operational data, and be subject to varying regional regulations, making it difficult to maintain consistent security policies and audit trails. The scale and heterogeneity increase the risk of vulnerabilities slipping through the cracks, leading to potential downtime or noncompliance penalties.

To address these weaknesses, customers tell us that they are adopting:

- Infrastructure-as-code and GitOps: Processes support automation of IT infrastructure for consistent, automated configuration and policy enforcement.
- Automated compliance monitoring and reporting: Activities detect and remediate drift.
- Open source frameworks and open standards: Examples including LFEdge and LFEnergy ensure interoperability and avoid vendor lock-in.

By embedding security and compliance directly into their core platforms, companies can reduce risk while accelerating innovation.

PUTTING AI AND ML TO WORK – SENSIBLY

Thinking beyond AI does not suggest the subject is unimportant. Quite the contrary. In industrial organizations, AI and machine learning are enabling predictive maintenance, real-time quality inspection, and energy optimization – just as a starting point.

However, challenges remain around data availability, quality, and the ability to deploy complex models on resource-constrained edge devices to monetize the AI economy. These challenges limit AI applications' scalability and reliability, especially in real-time edge environments where data is fragmented, unlabeled, or inconsistent. Additionally, deploying large models often requires trade-offs in performance, energy consumption, and latency — factors that directly impact the business case for AI monetization.

THE KEYS TO SUCCESS LIE IN:

- Data access and governance: Structured approaches for creating and enforcing policies that control access to data, to integrate operational technology (OT) data sources such as SCADA and PLCs with IT platforms
- Efficient AI techniques: For using semi-supervised or unsupervised learning, synthetic data, and transfer learning — and knowing when to use them
- Secure AI models: Rapidly updated, audited, and validated
- Continuous improvement: For retraining models centrally, with the aim of boosting accuracy and adaptability over time
- Optimized edge AI models: Lightweight, hardware-accelerated models (such as those leveraging Nvidia GPU support) that are deployed for inference at the edge, while offloading heavy training workloads to centralized data centers

As companies transition from pilot projects to production AI, a focus on incremental wins and strong business cases becomes essential to demonstrating ROI and building organizational momentum.

BRIDGING THE SKILLS GAP: THE HUMAN ELEMENT

Technology doesn't deliver value. People do. The convergence of IT and OT demands a workforce that understands both domains, along with new technology approaches including AI, cloud, and automation.

To succeed, companies must:

- Invest in training and upskilling for both IT and OT teams.

← TABLE OF CONTENTS

- Embed change management to overcome resistance and drive adoption as new technologies reshape workflows, decision-making processes, and the balance between humans and machines.

- Reimagine human roles to shifting from "in the loop" to "on the loop," where human oversight enhances machine autonomy.

Without a deliberate workforce strategy, even the most advanced technologies stall.

WHERE ELXR FITS IN

We are at an exciting inflection point in the industrial edge journey. There are opportunities to tame complexity with cloud-native integration and orchestration, to build security and compliance into the technology foundation (not as an afterthought), and to empower workforces to bridge the IT-OT divide.

Wind River is perfectly positioned to help you achieve those goals.

For example, by working with our partners, we extend what organizations can accomplish. eLxr Pro is a commercial-grade Debian Linux. It connects, orchestrates, and manages heterogeneous edge workloads while maintaining flexibility and scalability through partners such as Avassa. By combining Avassa's edge orchestration technology with eLxr Pro, organizations can manage diverse edge environments, including seamless orchestration of containers and virtual machines.

Another example: eLxr Pro takes advantage of the Zededa and NVIDIA partnership ecosystem to solve real AI workload challenges, from seamless AI model development and optimization to secure deployment and zero-touch management, across diverse edge environments.

Wind River is no stranger to security concerns in industrial environments. With eLxr Pro, companies can deploy minimal, hardened operating system builds, automate over-the-air updates, and integrate compliance monitoring to meet global standards such as NIST, General Data Protection Regulation (GDPR), and the upcoming EU Cyber Resilience Act.

Furthermore, Wind River is perfectly positioned to help industrial organizations up-skill their employees' tech knowledge, with eLxr Pro add-on professional services such as consultation hours, training, and security advisory services.

As the industrial automation market continues to grow, those who align technology, processes, and people are best positioned to thrive. With solutions such as eLxr Pro, industrial leaders are not just modernizing operations — they are shaping the future of resilient, intelligent, and human-centered industrial ecosystems.

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.

← TABLE OF CONTENTS

Real-Time Solutions at the “Cosmic Edge”

By Hans Weggeman, Field Application Engineer

NASA’s Artemis missions aim to return humans to the Moon, establishing a sustainable lunar presence. Advanced technologies for space stations, satellites, human surface mobility, and extravehicular activities (EVA) are critical for enabling astronauts to navigate and operate on the lunar surface. Responding to the harsh environment requires reliable, high-performance systems — and the industry is now shifting to more advanced computing architectures to support that requirement.

There are many challenges to developing technology for the space industry, including:

- Bridging legacy systems with new, AI-imbued technology and autonomous functionality
- Reducing volume, mass, cost, and power consumption of systems
- Handling project uncertainty given changing priorities (and budgets) for science and military space missions
- Achieving real-time hazard detection, navigation, and operational sustainability
- Integrating mixed-criticality workloads on a single platform

Addressing these challenges is critical to mission success and advancing space exploration

A NEW APPROACH

The IEEE Space Mission Challenges for Information Technology / Space Computing Conference, cosponsored by Wind River earlier this summer, delivered compelling insights into the future of embedded systems for space exploration. We presented on several topics, such as our partnership with Microchip on the High Performance Spaceflight Computing (HPSC) platform; VxWorks®; and native support for NASA’s flight software frameworks, including NASA cFS and F’, which ensure seamless integration with existing spaceflight systems.

The conference highlighted a fundamental shift in space computing architecture. Traditional approaches of deploying separate systems for different functions are giving way to consolidated multipurpose platforms that can handle everything from real-time hazard detection to AI-driven navigation systems. This consolidation isn’t just about efficiency; it’s about survival in an environment where size, weight, and power (SWaP) constraints are paramount.

Modern space computing systems seamlessly integrate AI/ML workloads alongside traditional real-time tasks at the edge. As a result, machine learning algorithms can run on general-purpose GPU hardware while maintaining real-time guarantees. That offers new possibilities for autonomous hazard detection, intelligent navigation, and adaptive system management — capabilities essential for operations on the lunar surface and beyond.

The conference reinforced that successful space computing platforms must be inherently scalable and future-proof. The ability to support and de-risk missions at various classification system for payloads (Classes A–D) demonstrates the versatility required for modern space exploration. The industry emphasis on cybersecurity and software interoperability ensures that these platforms can respond to emerging threats and requirements while maintaining the strict certification and reliability standards that space applications demand.

This is our core competency. Wind River has a long history of providing technologies for space missions.

WIND RIVER’S TECHNOLOGIES FOR SPACE

Relevant tools start with VxWorks, a deterministic, priority-based preemptive real-time operating system (RTOS) with low latency and minimal jitter, enabling mission-critical applications to operate reliably. VxWorks also supports AI/ML workloads on general-purpose GPU hardware for modern, scalable systems. It works with NASA’s core Flight System (cFS), a scalable and flexible software architecture to enable real-time data processing for immediate feedback, hazard detection, and decision-making.

Wind River® Linux, based on the Yocto Project, can be integrated into our Type 1 hypervisor, Wind River Helix™ Virtualization Platform, which enables mixed-criticality systems by consolidating safety-critical and non–safety-critical applications onto a single hardware platform. This ensures isolation, scalability, and efficient resource utilization.

The future of space exploration isn’t just about getting there — it’s about staying there, operating safely, learning about the cosmos, and continually pushing the boundaries of what’s possible in the harshest environments.

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.

← TABLE OF CONTENTS

Want to Learn More?

Check out these resources for more insights into the technologies Aptiv is demonstrating at CES 2026.

APTIV AT CES

Get details on the technologies that will be on display. Plus you can take a virtual tour of our pavilion after the show.

https://www.aptiv.com/en/ces-2026

APTIV INSIGHTS

Access white papers, articles, videos and other content throughout the year.

https://www.aptiv.com/en/insights

APTIV SOLUTIONS

Find out more about Aptiv's solutions powering the intelligent edge.

https://www.aptiv.com/en/solutions

APTIV INDUSTRIES

Find out more about the various industries served by Aptiv's businesses.

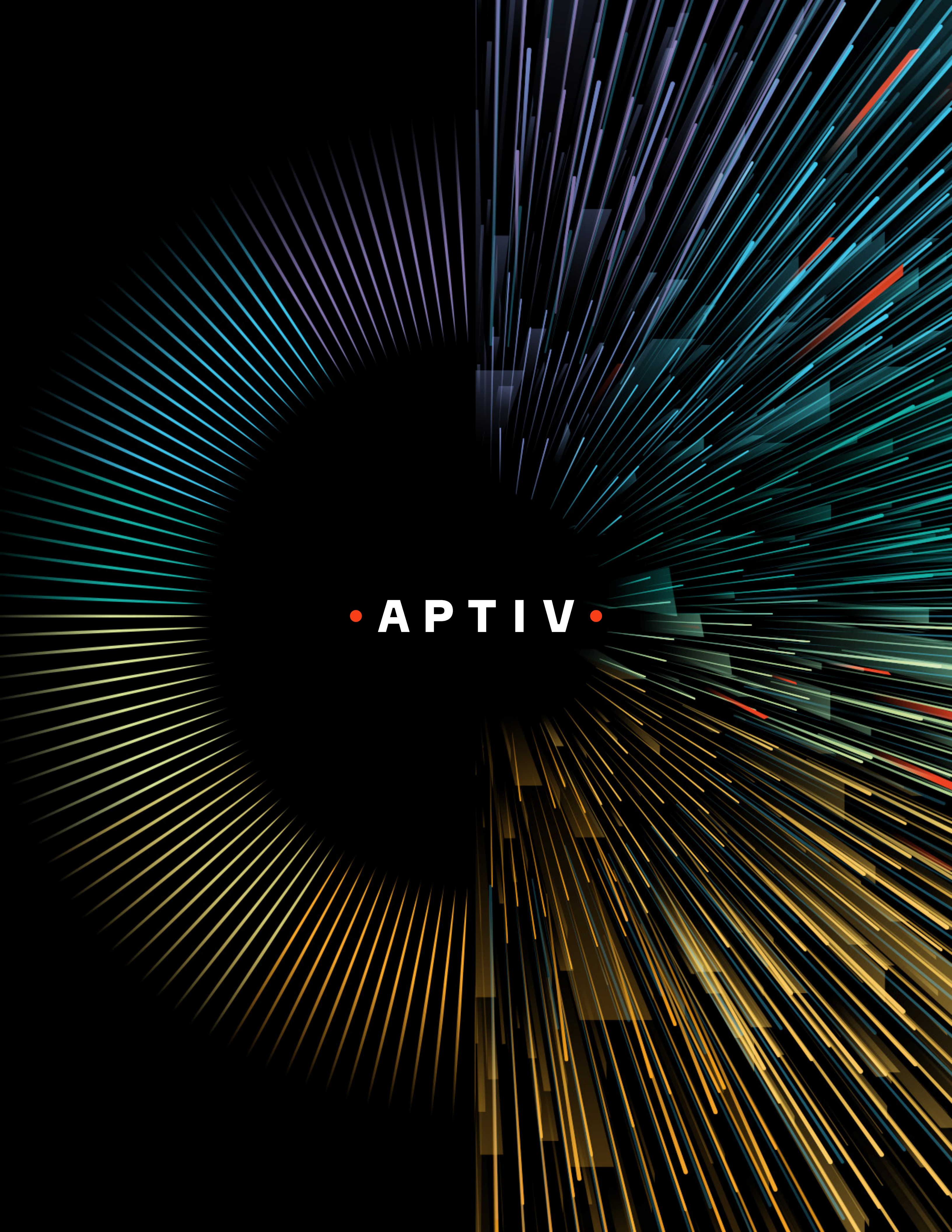
https://www.aptiv.com/en/industries

APTIV ON LINKEDIN

Follow Aptiv today for updates from CES 2026 and throughout the year.

https://www.linkedin.com/company/aptiv

← TABLE OF CONTENTS



APTIV