Building Next-Generation Software-Enabled Armoured Vehicles

Enabling Technologies for Digital Transformation of the Land Battlespace

WNDRVR

EXECUTIVE SUMMARY

Armoured vehicles which are purpose-built for mission-critical operations are reliant on control systems that provide deterministic behaviour to meet hard real-time requirements, deliver extreme reliability, and meet rigorous security requirements against evolving threats. Wind River® has the partners and the expertise, a proven real-time operating system (RTOS), software lifecycle management techniques, and an extensive track record to meet and exceed these requirements.

TABLE OF CONTENTS

NEW TECHNOLOGIES OPEN MARKET OPPORTUNITIES

Military armoured vehicles today differ markedly from early generations, as new technologies have expanded and strengthened operational capabilities. Autonomous and semiautonomous vehicle operations are enabled by faster processors, artificial intelligence (AI), more compact and energy-efficient computers, and scalable cloud computing. Sophisticated simulation software lets suppliers design and test system components even when these suppliers reside in geographically separate regions. Modern design methodologies, such as DevSecOps, have gained widespread adoption for embedded edge devices, simplifying the consistent development of secure, highly maintainable systems in a cloud-native environment.

Several factors drive armed forces to acquire modern armoured vehicles. Increasing geopolitical, low-intensity warfare incidents; the need for rapid deployment of forces in areas all over the world; and standardisation requirements (as part of alliances such as NATO) have all had an impact on vehicle acquisition.

Modernisation programmes are underway globally as leading countries with large defence budgets seek to bolster their capabilities, update or replace obsolete equipment, and deploy armoured vehicle fleets with technologies that increase mission readiness. These countries often lean toward bespoke solutions developed in collaboration with vehicle OEMs, technology experts, and mobility communication leaders. Smaller countries with restricted budgets are scanning the market for solutions that are less custom but capable of meeting urgent requirements quickly and effectively.

FUNDAMENTAL SYSTEMS IN A MODERN ARMOURED VEHICLE

Light, medium, and heavy armoured vehicles are typically equipped with essentially similar systems, as shown in Figure 1. The primary differences are the type and amount of armouring and the extent to which these vehicles have been engineered to resist damage from hostile fire, whether from rocket-propelled grenades, anti-tank weapons, armed drones, or other types of weaponry.

In a software-enabled armoured vehicle, these systems can be connected through a cloud platform. Applications (as well as mission data) are updated by OCI-compliant containers and provisions are in place that follow DevSecOps practices for rapid deployment and full automation over the system's lifecycle. Although cloud-native development, deployment, operations, and service are available today, the operational and maintenance cycles that characterise the military environment are not necessarily conducive to their use. It is not always possible or even desirable to perform a software update on a vehicle at the front line, for example, even though the capability may present an operational advantage.

Beyond the vehicle itself, which may be delivered by any of several specialty OEMs, there are the added systems that enable specialised functions, such as autonomous operation, communication within a cloud environment (mobile, edge, or multi-cloud hybrid), electronic control unit (ECU) consolidation, hypervisors, weapons control, self defence, and so on. These additions are usually handled by a traditional aerospace and defence (A&D) prime, often in partnership with system/subsystem suppliers and other specialised technology providers.

The deep experience Wind River has with large-scale systems for space exploration, avionics systems, industrial automation, electrical grid substations, and hybrid cloud deployments provides an ideal foundation for building next-generation software-enabled armoured vehicles.

Software-Enabled: The New Armoured Vehicle

The term *software-enabled armoured vehicle* covers a multitude of different roles and vehicle types, from infantry combat vehicles to armoured personnel carriers, from main battle tanks to mobile command stations; and vehicles with and without weapons, tracked or wheeled, and manned or optionally manned.

Software-enabled means that functions, and in certain cases even hardware, can be manipulated, enhanced, created, and managed by means of mechanisms based on software control. When an A&D system is software-enabled, its capabilities can evolve more easily, and new technologies can be more affordably integrated throughout the 20 to 40 years of operations that most A&D systems experience.

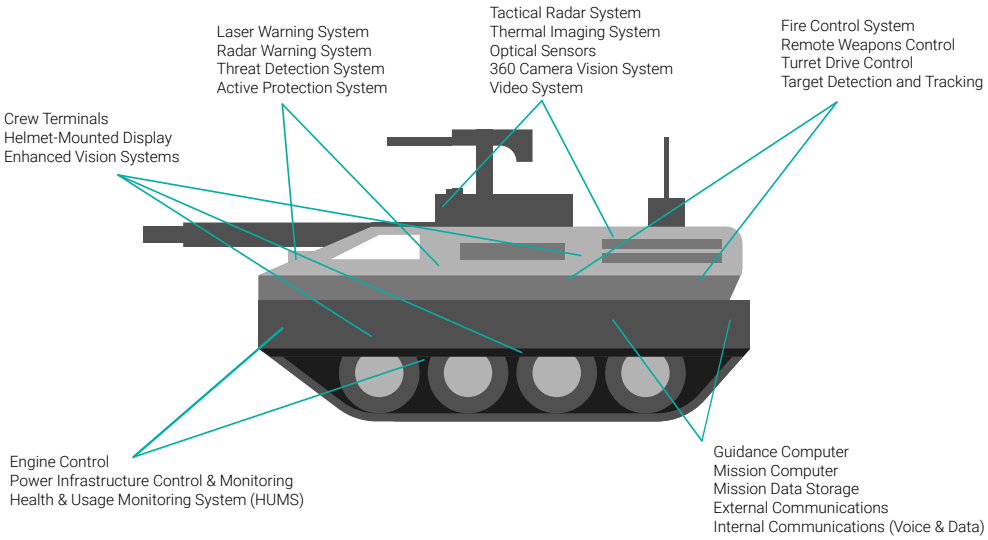

Figure 1. Primary systems in a battle tank

INCREASING INTEROPERABILITY THROUGH OPEN STANDARDS

With the expectation that land platforms will undergo numerous upgrades and modifications during operation over a decade or more of use, open standards–based architectures simplify platform design by minimising integration of components and defining a unified environment for subsystem deployment. By avoiding the costly and inefficient nonstandardised approach that has prevailed for years with military land vehicles, many key problems can be minimised or eliminated.

- Crew control and displays can be made more uniform, streamlining training, usage, and maintenance requirements.
- Power conflicts between platform components can be minimised.
- Data generated by the system can be analysed more effectively and exploited to improve platform operation and performance.
- The use of open architectures makes it easier and more cost-effective to design and integrate multiple electronic subsystems onto military vehicles.
- From crew displays with multifunction capabilities to control units based on a unified framework, important vehicle functions become more accessible and immediately familiar to vehicle operators.

The NATO Generic Vehicle Architecture (NGVA) STANAG 4754 ensures an open architecture approach for land vehicles and aims to provide interoperability across NATO vehicle fleets, standardising the power infrastructure, electrical, and electronic subsystems and the verification and validation process. NGVA enhances the operational effectiveness of vehicles, reduces integration risk of subsystems, and lowers the total cost of ownership across NATO nations. Key drivers for NGVA are:

- An agile mission platform
- Innovation and faster technology insertion
- Increased interoperability between systems
- Reduced lifecycle costs

The current version of NGVA addresses the communications mechanism between subsystems, using Data Distribution Service and a defined data model. It recognises that other standards may be used to define application execution environments, such as Future Airborne Capability Environment (FACE™) or European Component Oriented Architecture (ECOA). These would be nation-specific to fit in with other operational goals at the national level.

To improve software reusability and provide support for complex networked systems, ECOA was developed as an open specification. This framework for mission-system software includes components that operate in real time as well as those that are service oriented.

In the U.S., two open standards provide guidance for weapons system development and acquisition for the Department of Defence (DoD): the Vehicular Integration for C4ISR/EW Interoperability (VICTORY) and FACE, which is an example of the MOSA (Modular Open Systems Approach) strategy. These standards are becoming more closely aligned to strengthen interoperability goals.

FACE was originally designed for aircraft systems to make software portable and independent of real-time operating systems and safety-critical functions. VICTORY, developed as a hardware architecture standard, increased interoperability of armoured vehicle design and development, standardising the interfaces to vehicle systems and defining the in-vehicle network and on-the-wire-network for C4ISR/EW equipment.

Another U.S. initiative is for sensor standardisation. Sensor Open Systems Architecture™ (SOSA™) is a higher-level standard that aims to achieve commonality among sensors used. The guidelines

were established by the Open Group SOSA Consortium for use by command, control, communications, computers, and reconnaissance (C4ISR) systems.

From the perspective of operating system functionality, for developers of the applications running the control systems shown in Figure 1, the requirements of NGVA, ECOA, and FACE are well defined. With POSIX® and FACE compliance, Wind River operating system solutions fit comfortably into those standards, whether a hard real-time deterministic operating system such as VxWorks®, a Wind River Linux environment, or a hypervisor-based solution using Helix™ Virtualization Platform. The standard networking solutions accessible through Wind River OS solutions are suitable for meeting most interoperability issues. Unlike the scenario for aircraft systems, certification to specific standards is not necessary for NGVA. It is the responsibility of individual end users to perform any testing at the system level. Meeting the criteria of open standards is suitable in most cases to ensure software compatibility.

Volume VI of the NGVA standard covers safety aspects of vehicle systems, and as we shift toward autonomous vehicle operation, these safety requirements will increase. The NGVA standard references both the automotive safety standard (ISO 26262) and the industrial safety standard (IEC 61508).

THE UNIQUE ADVANTAGES OF AUTONOMOUS MILITARY VEHICLES

Autonomous, semiautonomous, and optionally manned military armoured vehicles each have a role in digitally transformed defence implementations, and the technologies within each area are being refined at a rapid pace. It is possible to envision a time, not far in the future, when military armoured vehicles will perform missions such as supply runs, reconnaissance expeditions, or terrain surveys without needing personnel on board. This could be a distinct advantage in situations in which the lives and health of personnel are at risk because of potential enemy actions. Creating a vehicle that is optionally manned can be valuable in instances involving missions that have one or more individuals on board with the understanding that the vehicle is also capable of being operated in fully autonomous mode. In addition, by enabling greater autonomy in vehicle operations, the number of crew members required to complete a mission can be reduced, thereby lowering overall risk and cost for an entire fleet.

The recently announced partnership between Wind River and Aptiv brings a wealth of experience around autonomous and semiautonomous vehicle operation to engagements, dovetailing with Wind River experience in software-enabled architectures.

DEVSECOPS PROVIDES INNOVATIVE WAYS OF RETHINKING VEHICLE DESIGN

The continuous integration/continuous delivery (CI/CD) workflow that gained popularity as DevOps practices matured has been extended to encompass security provisions more deeply with DevSecOps. Following the principles of DevSecOps is a proven method of strengthening security, starting at the very earliest stages of design to mitigate potential security vulnerabilities and develop systems at each level that protect against malicious intrusions and hacking threats. Wind River has adopted DevSecOps practices into development pipelines and integrated these underlying principles into toolsets for use by the development community to collaborate and build complex systems involving multiple organisations and wide-ranging goals.

A modern military land vehicle is comprised of many interlocking subsystems, with software functioning at different levels for controlling operation of the vehicle and communication with command-and-control centres. The cloud-native toolset provided by Wind River Studio supports development processes that follow DevSecOps principles, integrating new software releases into the main body of code systematically and with rigorous testing available at each stage of the pipeline. Building secure military land vehicles requires the collaborative work of many different teams, from the OEMs who construct the physical vehicle to the developers who create the apps to control the vehicle. Robust security is a team effort, furthered by a development environment that supports DevSecOps practices.

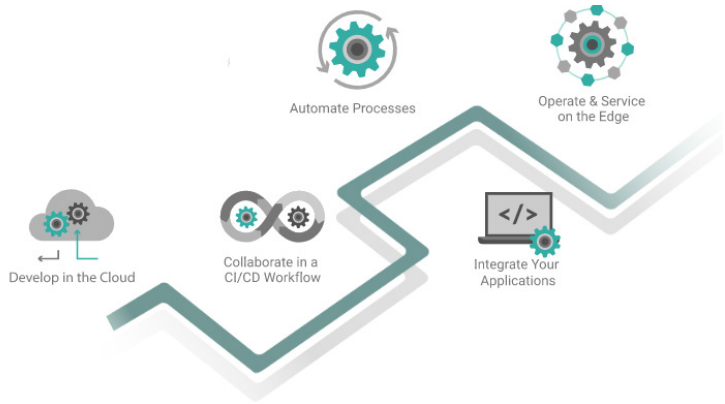

Figure 2. Studio development processes support DevSecOps principles

Once vehicles have been procured and become active in the field, fleet management and daily operation are important concerns. The DevSecOps environment proves invaluable in managing security patches and software updates to change the various mission systems. The status of each vehicle in the fleet inventory can be monitored and verified to ensure that security is up-to-date and systems are functioning well for the intended missions. Management of fleets

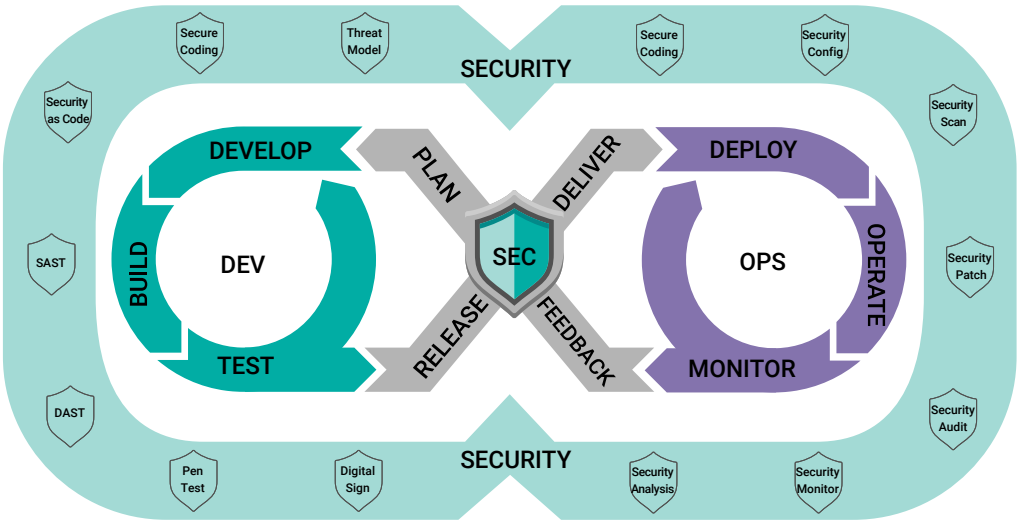

Figure 3. A DevSecOps workflow includes ongoing security analysis and testing

can be a risky proposition without a system which ensures that there are no weak points in the system security perimeter, or attack vectors which have not been mitigated.

A practice that has proven useful in avionics can also be applied to military vehicles. Aircraft equipped with an internal cloud server can use containerised applications for updating and maintenance; this kind of software architecture can also be used in military vehicles in the field. Technology developed by Wind River and Aptiv could make it possible to have a central management computer in a mobile cloud configuration that can update, on the fly, other computers on different vehicles. When there is persistent connectivity to headquarters, a central management computer can deliver the latest containerised applications that are ready for the next update through the mobile cloud or other means.

The Studio environment makes this type of operation accessible and offers opportunities to systematically control and update military vehicles deployed on missions. This innovative approach could have wide application in the A&D sector, beyond the operator example provided.

ACHIEVING OPTIMAL FLEXIBILITY IN THE FIELD

The trend toward software-enabled systems is one that appears to be accelerating as end users realise that the flexibility offered by this approach has numerous benefits and makes it possible to adapt a system or machine to multiple uses. When applied to armoured vehicles, a single configuration of a vehicle can be tailored to one type of mission and then reconfigured through software to perform other functions that address new or changing mission requirements. In this way, a single type of vehicle can be reconfigured as needed to adapt to changes in field conditions, new requirements, mission priorities, and unexpected situations as the need arises. Rapid field updates are possible either through a traditional cloud network, if available, or through a mobile cloud in environments in which communication is sporadic or nonexistent.

Figure 4. Studio spans the lifecycle of intelligent systems

Shortening Long Development Cycles with Simics

An invaluable tool throughout the development process of many types of complex systems, Wind River Simics® allows teams to build and test simulations of systems within a cloud-native environment — without needing the actual hardware present. The toolsets available through Studio can help design, develop, and deploy the framework for creating the simulation and manage collaboration with contributors and organisations involved in project development, some of whom may be building subsystems that will operate within a complex system.

By automating the processes for integrating and deploying components in a simulation of the final system, much of the difficult development work can be accomplished without the need for hardware prototypes. Geographically separated engineers and developers can work together on a final design, test and validate individual components for interoperability, perform regression testing, confirm software compatibility, measure solution performance, and verify that requirements have been met. This can shorten development cycles by eliminating hardware supply chain delays and detecting design problems before investing in actual hardware prototypes.

Software users who are not familiar with the depth and sophistication of Simics may not realise the full scope of time savings and development acceleration that is possible with this type of simulation and a cloud-native development environment. Technology often changes during the course of building any type of system, for example. However, even if the architecture changes during development, Simics and a cloud-native development environment let the project continue. Prototypes can be developed with the latest configurations in place. Migrations to different environments can be accomplished easily even as the design progresses.

Delivering Maximum Safety and Security in a Software-Enabled Vehicle

Simics also enables teams to subject components and systems to multiple forms of security testing. These simulations can be used to discover vulnerabilities, explore potential attack vectors, and institute layered security measures that provide a high degree of security. Components developed by multiple teams can be tested in a secure environment to explore design concepts and ensure interoperability before hardware prototypes are built.

In a simulated environment in combination with the latest container technology, the discovery of vulnerabilities — whether new malware, a newly uncovered cybersecurity threat, or weaknesses in applications or operating systems — can lead to quick action. Patches can be made using containers, often without taking the deployed system out of service. Wind River has invested considerable energy and effort in advancing and refining container technology and continues to lead in scenarios in which mission-critical, fail-safe operation is paramount.

Capitalising on the Advantages of Electric and Hybrid-Electric Drive Technologies

In response to the rising threat of climate change and to gain operational advantages for future vehicle fleets, plans are underway by the DoD — in cooperation with the auto industry — to introduce electric and hybrid-electric drive technologies into large segments of the military. Currently, some 170,000 non-tactical military vehicles are already in use on military bases. This is the second-largest deployment in the U.S. federal government, trailing only the U.S. Postal Service.

Fuelling electric vehicles in the field presents a significant hurdle for the military. In a *Defense News* article,[1] U.S. Army Brigadier General Glenn Dean summarised the problem by saying, "The huge challenge at the end of the day: It takes X amount of energy to move your vehicles to point A to point B. Then you need X amount of energy to move again. Where does it come from? I can drive a Tesla 300 miles, but I'm expecting a Tesla charging station at that point. Where are those charging stations on the battlefield? Do you have to bring them with you, or are you going to expect them to be there?"

Armoured vehicles, of course, tend to be very heavy and often need to travel very fast, which brings up engine requirements that are more demanding than those of the urban environment — even when considering hybrid-electric vehicles, whose engines can usually supply much of the needed charging. Despite the challenges, however, military planners are actively scoping the possibilities and beginning to prototype. The potential exists for vehicles that not only have a high-efficiency, self-sustaining energy source but that operate with minimal noise and low heat signatures.

Control systems specifically for electric and hybrid vehicles will need to be designed, an area where Wind River could make valuable contributions to advancing the technology. Communication systems

1 *Jen Judson, "Is the Army Warming up to Electric Vehicles in Its Fleet?" Defense News, June 2021*

to identify charging stations, vehicle battery status, and lifecycle stage in the field, as well as other resources valuable to maintaining electric vehicle fleets, would be useful. The use of robotics in the systems of software-enabled electric or hybrid-electric armoured vehicles is another area for exploration.

As the defence sector more actively explores the possibilities of tactical vehicles with electric propulsion, innovative examples have been appearing with greater frequency at industry events. For example, at the Eurosatory trade conference in Paris in early June 2022, vehicle makers exhibited innovative equipment, including the Arquus Scarabee light armoured vehicle, with a fully hybrid powertrain; and the eight-wheel drive FFG Genesis, an armoured personnel carrier. The event also displayed the DURO-e, an all-terrain tactical vehicle that was fully electric and featured battery or fuel cell power options. The vehicle was codesigned by General Dynamics, Magna Powertrain, and Phi-Power AG.

Surveying the state of developments in an article for *Defense News*,[2] Vivienne Machi noted, "Gone are the days when military vehicles simply need to roll. Now, they must come equipped with complex communications systems, radars, lasers, jammers, and other electronic systems, turning battlefield rides into mobile power stations."

CONCLUSION

Technologies are nascent for widespread adoption of software-enabled armoured vehicles, but advances are taking place on all aspects of implementing the vision at a rapid pace. Autonomous and semiautonomous operation of vehicles is within reach, and Wind River is partnering with companies that have a clear vision and the innovative mindset to realise the promise of this next generation of vehicles. Edge computing and cloud networking have proceeded at an equally rapid pace, and military aircraft are beginning to deploy systems that rely on the cloud for communication. The solid benefits and versatility of software-enabled machine technology will likely hasten military organisations in becoming adopters and proponents, as armoured vehicles based on this approach move on from the planning stages and are built in increasing numbers worldwide.

2 *Vivienne Machi, "Vehicle Makers Court Europe's Military with Hybrid, Electric Rides," Defense News, June 2022*

Additional Resources

Learn more about Studio, the first cloud-native platform for the development, deployment, operations, and servicing of mission-critical intelligent edge systems.

To explore the ways in which VxWorks, the Studio real-time operating system, provides RTOS capabilities for embedded systems, see VxWorks: Redefining the Role of the RTOS.

Learn how Simics can expose cybersecurity threats and test complex system scenarios for those designing and developing systems for military vehicles.

To learn more about certification of safety-critical applications, visit VxWorks Safety Platforms.

WNDRVR