IDC ANALYZE THE FUTURE

IDC ANALYST CONNECTION

Sponsored by: Cybellum

As automotive manufacturers continue their pursuit of the software-defined vehicle, they must recognize that cybersecurity approaches, processes, and tooling must evolve to be increasingly holistic, centralized, and always on.

Extending Digital Twins into Cybersecurity to Evolve Vehicle Security and Compliance

February 2021

Questions posed by: Cybellum

Answers by: Matt Arcaro, Research Manager, Digital Automotive and Transportation Strategies

---

Q. What advice do you offer automotive organizations as they look to improve vehicle cybersecurity visibility and performance?

A. When organizations look at ways to improve vehicle cybersecurity, they must first realize that there is no silver bullet that will solve all their challenges. Cybersecurity really encompasses a dynamic spectrum of decisions and actions that require constant vigilance, investment, and evolution. IDC recommends that automotive organizations look at cybersecurity as the overlap and intersection of two key foundational pillars: process and technology.

- The process pillar represents the organization, people, and cultural elements of cybersecurity that need to be designed, deployed, and nurtured. These processes define how and where cybersecurity should be viewed and implemented internally. They also influence how cybersecurity affects the conversations, requirements, and work products of upstream and downstream partners. An effective cybersecurity process requires that all contributing organizations work together to ensure that all aspects of the vehicle life cycle are deployed and remain safe and secure. As organizations look at deploying these processes, they should give careful consideration to avoiding one-time assessments because vehicle software and components need to be continually evaluated, maintained, and remediated throughout their life cycles.

- The technology pillar represents the capabilities and solutions that are designed and deployed to protect vehicle systems from unwanted access or misuse. IDC recommends that manufacturers actively evaluate and engage with the security technology ecosystem. While existing providers and new entrants are leveraging best practices from other industries and domains, it's important to make sure that they address the unique needs of vehicle product security. One such example of innovation is extending the concept of a digital twin into automotive cybersecurity.

Q. Can you elaborate on the concept of a digital twin for cybersecurity? What benefits could it provide to automotive organizations?

A. Digital twins are updatable models that represent a nearly identical, virtual copy of a process, a device, a component, an environment, and/or a system. They are increasingly used to introduce transparency and speed to decision making as well as to determine the impacts of changes or updates without the risk, cost, and time spent on performing the analysis on the host. In the automotive industry, the digital twin concept is being applied to cybersecurity. An organization can now develop a complete, referenceable, and updatable twin of a vehicle's software for one-time or continual assessment and monitoring. Looking at cybersecurity through a digital twin's aperture may help deliver benefits such as:

- Integrating the collection and maintenance of all underlying software metadata in one place, including versioning and configuration
- Simplifying the process to design and enforce cybersecurity requirements and policies across a complex manufacturer, supplier, and service provider value chain
- Incorporating vulnerability detectability and traceability capabilities that identify dependencies on a specific system and/or vendor
- Creating a common output that can be shared and referenced by approved third parties
- Providing a single entity by which all vehicle systems can be continually assessed at stages from design to post-production

Q. Do you see opportunities where digital twins for cybersecurity could help with automotive industry challenges?

A. Opportunities exist for the digital twin–based approach beyond just satisfying technology requirements. In particular, it could help support the greater automotive organization in considering and incorporating cybersecurity end to end across the business. Using a digital twin model could help with:

- **Simplifying the process for compliance validations and audits.** The digital twin requires that an organization consider and build an extensive pipeline of data elements into the tooling to be successful. This not only accelerates the need for organizational alignment and cooperation but also supports trust being built around a single source of truth.

The digital twin–based approach could help support the greater automotive organization in considering and incorporating cybersecurity end to end across the business.

- **Reducing the complexity of managing incidents.** A key challenge in the "modern" automotive software approach stems from understanding the impacts and susceptibility of vulnerabilities across the sheer number of potential parties. The digital twin provides a unified way to report, track, and identify the impacts of such an assessment, including the party responsible for the response and the fix.
- **Facilitating cybersecurity differentiation and ecosystem collaboration.** The digital twin model allows automotive organizations to harness vehicle data internally as well as externally. In this way, by controlling the access and sharing of data, automotive manufacturers are able to communicate challenges and learnings as well as innovate with suppliers, auditors, and/or service providers more quickly and easily.
- **Building on top of a single source of cybersecurity truth.** Although digital transformation (DX) initiatives remain ongoing and widespread throughout automotive organizations, very few will result in a comprehensive, indelible source of truth for their respective focus area. A digital twin for cybersecurity can be a key foundational input (or output) to build around as an organization looks to expand these initiatives beyond individual "domain" boundaries.

Q. In what ways are cybersecurity regulations and standards evolving in the automotive industry? How would a digital twin for cybersecurity help manufacturers address these requirements?

A. As the automotive industry continues to increase the amount and role of software in its vehicles, there has been widespread recognition that regulations and standards have been unable to keep up with the speed of technology innovation and adoption. Although no standard can fully address and mitigate all the risks of diverse software design and deployment approaches, the automotive industry has come together to position two comprehensive, modern, and complementary vehicle cybersecurity initiatives: the ISO/SAE 21434 standard and the UNECE WP.29 regulation.

Digital twins represent a virtual replica of vehicle components, systems, and/or devices, making them a great option for manufacturers looking to standardize a universal approach to adapt to ISO/SAE 21434 and UNECE WP.29. This includes leveraging the digital twin to capture the complex supplier software and system inputs needed to perform cybersecurity assessments, track and identify issues and vendors, and test and implement any fixes needed.

In addition, these tools can help automotive organizations address requirements for continuous monitoring of cybersecurity events, including assessing their impact upon on-road, deployed vehicles via repeatable, automated approaches.

Further, organizations may use a security digital twin, as well as interfacing cybersecurity tools, as the documentation and audit trail for regulatory compliance, including supporting ongoing reporting and assessment needs.

Q. What best practices should automotive organizations be aware of as they perform their due diligence of evaluating digital twins for cybersecurity?

A. IDC engages with a broad range of diverse automotive organizations and suppliers. Although these organizations may not have the same ambitions or hierarchy, IDC has found common traits and best practices that they can utilize to understand and evaluate new technologies such as the digital twin for cybersecurity. These include:

- Ensuring that product security teams incorporate the requirements and perspectives of a diverse group of organizational (i.e., domain-specific) and comprehensive vehicle life-cycle (i.e., from design to post-production maintenance and support) stakeholders. This approach will help an organization identify, document, and prioritize cybersecurity challenges and limitations as well as enable it to effectively baseline the benefit of introducing new technologies and capabilities, including digital twins.
- Understanding how and if a digital twin for cybersecurity can fit alongside an organization's existing frameworks and processes. For example, the centralized approach and visibility that the digital twin can provide should introduce efficiencies and optimization for vulnerability management. Additionally, it can reduce the complexity to integrate with back-end IT systems and tools related to product life-cycle management (PLM), software development life-cycle (SDLC), asset management, and over-the-air (OTA) updates.
- Looking to future compliance standards and regulations, including ISO 21434 and UNECE WP.29, to help identify where a digital twin for cybersecurity can help satisfy these requirements. The holistic nature of these standards will force organizations to pursue centralized technology solutions as well as process changes to maximize their adoption and use.
- Evaluating a digital twin for cybersecurity fit with an organization's short- and long-term goals. As part of their analysis, organizations typically focus on how a digital twin can help with today's pressing vehicle security requirements, including vulnerability and gap analysis. This needs to change as technologies such as digital twins will deliver increasing value as new software-driven technologies and architectures are introduced into vehicles. In many cases, adopting a digital twin–based approach in the near term will help organizations gain control, add predictability, and help streamline these advancements.

About the Analyst

Matt Arcaro, *Research Manager, Digital Automotive and Transportation Strategies*

Matt Arcaro is a member of IDC's Internet of Things (IoT) and Government Insights practices, leading its next-generation automotive and transportation research and thought leadership initiatives. In this capacity, Matt advises private and public sector clients on strategies that maximize the benefits of new and evolving technology, digitization, and networking. This includes an increased focus on the areas of intelligent transportation systems (ITS), emerging standards and regulation, connectivity and data sharing, mobility as a service (MaaS), fleet management, vehicle autonomy, electrification, cybersecurity, and go-to-market strategies and business models.

MESSAGE FROM THE SPONSOR

Cybellum enables OEMs and their suppliers to develop and maintain secure automotive products.

Our Cyber Digital Twins platform provides comprehensive visibility into automotive software, revealing their make-up, characteristics and the context in which they operate. All from binary files, no source code needed.

It exposes hardware architectures, operating systems, configurations, control flows, API calls, SBOM, licenses, encryption algorithms and keys, hardening mechanisms and more – generating an accurate digital replica - a Cyber Digital Twin - of every vehicle component.

Armed with such a deep understanding of vehicle software, Cybellum automates vulnerability management, compliance validation, continuous monitoring and incident response, minimizing risk to your customers and your organization.

Cybellum provides your product security team and PSIRT with the visibility, context and agility needed to focus on the most relevant and pressing cyber threats, trace their origin across the supply chain and quickly mitigate them, during and post-development.

Learn more about at ***www.cybellum.com***

IDC Custom Solutions

IDC Research, Inc.

5 Speen Street
Framingham, MA 01701, USA

T 508.872.8200

F 508.935.4015

Twitter @IDC

idc-insights-community.com

www.idc.com