Streamlining Global Automotive Cybersecurity Governance to Accelerate Innovation, Assurance, and Compliance

By Josh Kolleda

30 April 2025

Introduction

The dynamic and interconnected world of automotive cybersecurity presents unique challenges and opportunities for organizations managing multiple vehicle brands. Developing well-defined, collaborative organizational practices is crucial for enhancing operational efficiency, ensuring safety, and fostering shared technical innovation, all while preserving the unique identity and value proposition of each brand. A core concept to enhancing automotive cybersecurity assurance and compliance is ensuring the necessary level of authority, resource allocation, and opportunity to influence decision-making at the global C-level.

In current times, global corporations own and operate families of automotive brands under a single umbrella. Stellantis is a great example. Fourteen automotive brands and two mobility companies with operations in more than 30 countries and customers in more than 130 markets – all under a single corporation.1 While Stellantis is clearly one of the largest examples, many other brands fall under single multi-national corporations (e.g., Volkswagen, Toyota, GM, Geely, Tata).

Merging and acquiring brands is typically an effort to gain market share across regions, gain production efficiencies, acquire innovative technology, and ultimately make more money. Part of this strategy is maximizing the reuse of architectures and components across models, makes, and even completely different automotive “families” in an effort to increase economies of scale. As automotive cybersecurity standards and regulations

have emerged, with different regulatory mandates across regions (e.g., no actual mandate in the U.S.), these global corporations are challenged to ensure adequate cybersecurity engineering practices are met while rolling out common platforms that may offer varied features to meet customer desires along with meeting specific safety regulations. For example, the U.S. is not beholden to UN R155 and there is no cybersecurity focused Federal Motor Vehicle Safety Standard (FMVSS). However, the automakers still follow ISO/SAE 21434, the Department of Transportation National Highway Traffic Safety Administration (NHTSA) has published "Cybersecurity Best Practices for the Safety of Modern Vehicles," and the Department of Commerce - Bureau of Industry and Security has issued a final rule on "Securing the Information and Communications Technology and Services Supply Chain: Connected Vehicles" which will prohibit transactions of select vehicle hardware and software from China and Russia.

One could think of these challenges in line with the subject of quality within manufacturing or functional safety from decades ago – disjointed and sometimes competing governance, processes, and practices across siloed regions and even within region when departmental objectives and metrics are in conflict with a limited budget to address design requirements. So, cybersecurity leaders and teams at the global corporate level and within the brands that fall within these corporations are left with the daunting question:

How do I more efficiently manage automotive cybersecurity assurance across a global business with multiple vehicle variants, regulations, cultures, and siloed teams?

It is imperative to balance innovation with security assurance and securing platforms by design while also designing and preparing for verification and validation so you can prove the efficacy of your security concepts and controls. High levels of assurance do not necessarily arise from a security engineering framework that simply produces the work products from ISO/SAE 21434 or ISO/SAE 24089. Instead, the level of assurance depends more upon how effectively the policies/processes/systems that support the development and creation of these work products apply foundational security principles. As OEMs and suppliers seek to implement new technologies, they will inexorably be implementing new security strategies which in turn need new accompanying processes and tools to be developed, implemented, and then themselves validated before being integrated into the V&V environment. We are seeing more vehicle feature and type release delays with V&V becoming an increasingly large hurdle, both from a functional and security perspective, and obviously, no one wants security to be the cause of those delays. There are also inefficiencies and rework when working with multinational corporations that have multiple vehicle brands, even when reusing platforms and components. The early and systematic integration of cybersecurity processes, which should include peer and third party review, not only enhances vehicle security but also leads to significant efficiency gains. These gains are seen in reduced development times, lower costs due to preemptive security measures, fewer recalls or security breaches post-launch, and enabling new and more dynamic features.

Challenges to Assurance in Global Automotive Corporations

While automotive cybersecurity standards and regulations have come a long way over the past 10 years (from nothing to SAE J3061, ISO/SAE 21434 and ISO 24089, UN R155 and R156, NHTSA Automotive Cybersecurity Best Practices, etc.), OEMs and suppliers are still working through optimizing internal policies, processes, and procedures to operationalize these standards and document compliance efforts. Also, while UN R155 is a formal regulation within the EU and essentially adopted by much of the world, automotive cybersecurity is not formally regulated within the US (one of the largest vehicle markets in the world); although, NHTSA has released cybersecurity best practices and there are Federal rules that impact over cybersecurity posture and the supply chain. Also, China (the largest vehicle market) does not formally subscribe to R155. Instead, China developed its own automotive cybersecurity standards and regulatory framework (GB 44495, Technical Requirements for Vehicle Cybersecurity), which is comparable to UN R155, R156, and ISO/SAE 21434, in which OEMs must comply to sell vehicles.

These regulatory differences across regions create competing priorities or divergent efforts within a global OEM. At worst, from an assurance perspective, some regions may simply take a less rigorous assurance approach – "Why would I spend resources on something that is not regulated or enforced?". At best, each region (including US-based operations) is working within the spirit of the regulations and standards, but resources are wasted on duplicated workstreams (e.g., pen testing the same ECU in its entirety in different regions, rather than focusing on a single test with differentials testing on regionally based features).

There are also the standard organizational challenges inherent within any multinational corporation. These challenges can be amplified in some of the EV and ADS start-ups as they race to become first (or second/third) to market. Non-exhaustive examples:

- **Cultural Differences and Trust Gap**: Departments in different regions (or even within the same region) lack visibility into each other's development efforts. "I'm finding issues with code created by another department across the world. Who's the ultimate authority to address these issues?"
- **Organizational Silos**: For example, automotive engineers focus on functionality and safety, while security engineers emphasize protection, detection, response, etc. Bridging this gap is crucial. There may not be security controls implemented based on the feature's initial use case. There should be multiple layers of analysis ensuring that the feature is necessary to do a defined task, adequate security requirements are applied to prevent abuse, and that a user with legitimate credentials cannot leverage the feature in an unintended manner that could have a significant impact to safety, privacy, etc. "Yeah, this works, but there are use cases where a threat actor could leverage these 'features' for malicious purposes. This isn't secure so it's not safe."
- **Budget Constraints and Funding Alignment**: Pressure to minimize costs often results in underinvestment in cybersecurity. There may also be a fundamental mismatch in the design of the organization and allocation of budget. For example, budgets may be aligned to vehicle platforms and programs that use shared

components. “Which program should set aside part of their budget to fund assurance activities related to those shared components? I don’t want it coming out of my program funding.”

- **Lack of Qualified Staff**: It’s no secret that there’s a shortage of cybersecurity professionals in general. People with both automotive experience and cybersecurity expertise make this an even more niche career field. “I know what needs to be done in principle, but I don’t have the expertise to complete the work and I can’t hire people with the necessary experience and expertise.”

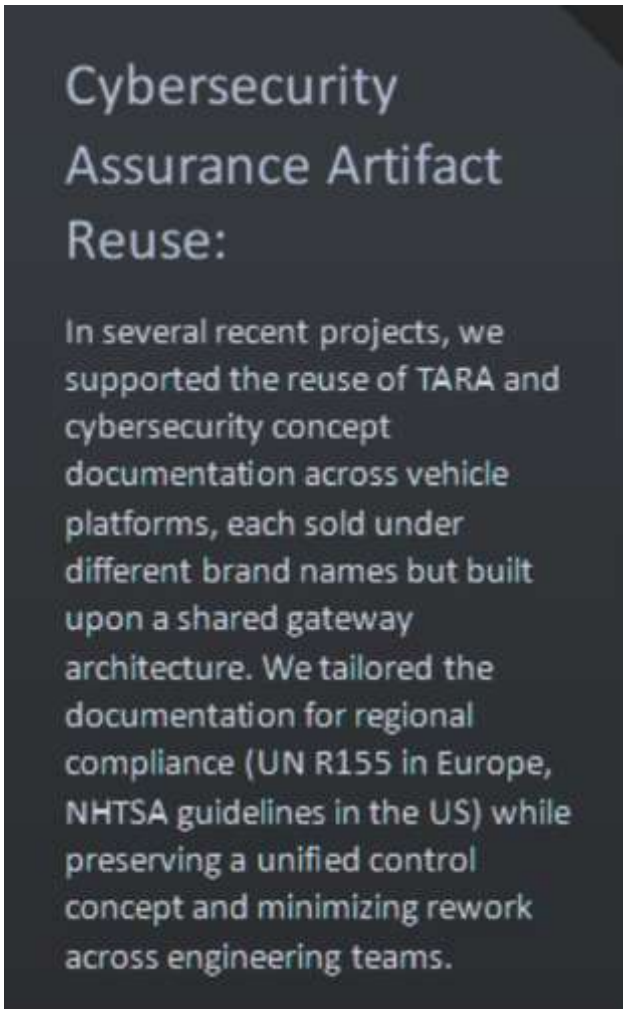
Reimagining Cybersecurity Governance to Increase Efficiencies

Centralizing leadership and accountability of security governance and process (or specific functions of security engineering oversight) has many benefits to an organization. However, the actual benefits will depend on the level of commitment to designing and implementing these changes in a manner that is palatable to the individual brands that make up the multinational corporation. Change is hard and we cannot forget this during any effort to transform the way an organization conducts its business.

Reimagining cybersecurity governance should drive down costs and increase efficiencies. Yes, there will be some additional required resources upfront to implement changes along with a short-term drop in efficiency (this is natural for any significant change in an organization), but the long-term cost reduction should be significant. Non-exhaustive examples:

- **Higher-level Security Champions and Advocates**: A global automotive cybersecurity function can advocate for assurance needs within the highest levels of business – similar to safety and quality.
- **Cybersecurity Terms within Contractual Agreements**: Where possible, this globally integrated department can set rigorous Cybersecurity Development Interface Agreements (CDIAs) to manage risk and align responsibility and accountability (along with the associated cost). Include requirements for design documentation and source code from suppliers potentially even through escrow, although this may require significant negotiation as it is a departure from the status quo.
- **Funding Streams for Cybersecurity Assurance**: Reengineer processes and governance of funding for cybersecurity aligned to data flows, features requirements, component, system, platform, and then vehicle. We are now seeing Software Defined Vehicles and architectures that are designed for change and dynamism during operation and throughout lifecycle states. Because of this evolution, it’s recommended to start thinking from a data flow and feature requirements perspective. A new framework such as this should help with homologation efforts and mitigate conflict among platform programs as the funding should come from a centralized cybersecurity budget.

- **Cybersecurity Assurance Artifact Reuse**: Develop once and reuse/tailor as necessary based on regional differences. Where appropriate, reuse Threat Analysis and Risk Assessments (TARAs), Cybersecurity Concepts, etc. across shared components in different brands.
- **More Efficient Testing**: Test core applications and components once and focus on differentials for regional variants, maximizing the Return-on-Investment for internal and third-party assurance support. This should result in less retesting, defects, warranty claims, and recalls.

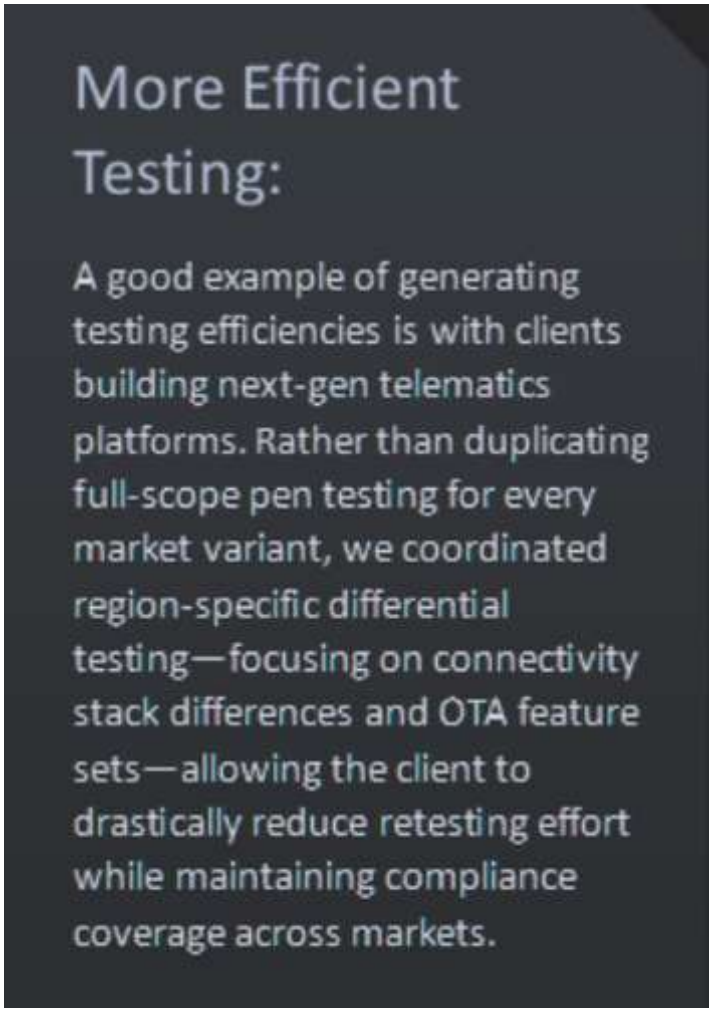


How do I transform and implement a global automotive security assurance program that will bring about lasting change and improvements?

This requires whole separate functional disciplines of “softer” skills (e.g., strategic planning communications, organizational design, change management, program management) where people spend their whole careers. Initially, it starts with leadership buy-in and making it a business priority from the top-down. Also, nothing will happen without the proper alignment of resources (e.g., people, funding, incentives, etc.). Leadership must champion cybersecurity priorities and allocate resources accordingly. Finally, leaders must build trust to enable change. These are

some key concepts and activities to consider (again, non-exhaustive and the activities will differ based on each OEM).

- **Stakeholder Engagement**: Without the right cybersecurity (and other functional) stakeholders across brands providing input, the new global strategy and organizational changes will fail. The people impacted by the change must have input. They have been doing the work and know the pain points, along with recommendations to address them. They must also be encouraged to maintain an open mind when solutioning.
- **Organizational Design**: Set the strategic vision, goals, and objectives of the global automotive cybersecurity assurance function. Analyze the existing organizational structure and consider hierarchies and reporting lines. Examine the people, process, and technology of the cybersecurity functions. Study the communication channels, decision-making processes, and incentive systems (or lack thereof).
- **Cybersecurity Policy and Process Reengineering**: Based on the new organizational architecture design, assess the policy and process changes necessary to successfully implement that change. Determine the current policy and process impediments to implementation and change them. As much as possible, align policies and processes to meet the requirements of the relevant automotive cybersecurity standards and reference regional deviations.
- **Change Management**: Employ the same stakeholders as the trusted champions of this change across the brands and individual cybersecurity teams. They will need to help explain the why and how this is happening along with guiding the rest of the business through implementation with support of global leaders. Create and deliver training to empower teams to take ownership of processes. Establish metrics to track effectiveness and adjust the strategy as appropriate.
- **Strategic Communications**: Determine the stakeholders impacted by the change and tailor communications to address their needs and concerns. Craft concise, consistent, and impactful messages that convey the purpose, benefits, and urgency of the change. Choose the appropriate delivery channels (e.g., emails, town halls, intranet) to reach different audiences. Ensure ongoing communications to provide regular updates, address questions, provide clarifications, and create feedback mechanisms.
- **Technical Program Management**: Through the entire transformation, global and regional technical program and project management is imperative to keep workstreams moving in accordance with the strategy. These PMs must collaborate with technical security leaders to ensure the efficacy of the activities. Given the significant effort of, for example, tracking component reuse and differentials testing across brands and models, TPM will also be a key function for continued operations.



Where do I start if I don't want to take on that level of change?

It is perfectly reasonable to think about the level of effort required for effective organizational change, and think, "No way. We don't have the resources to execute that."

Start with a pilot program focused on a component or platform

Start small and pilot this type of change at the initiation and scoping of a new component across models (e.g., a shared telematics control module or gateway module) or maybe a new vehicle platform (e.g., a new electric or automated vehicle platform architecture). Why at the beginning? Ensuring security is fully established in the product development cycle can A) help ensure that any weaknesses or limitations are documented (if they can't be remediated) or remediated in advance, B) allow conversations around security as an enabler – what new functionality/ features could we support if the component had XYZ property?

Make sure to establish metrics, regular internal reviews, and, very importantly, the opportunity to fail but fail fast and course correct. Document lessons learned and iterate on another component, platform, or enact the longer-term change across a global organizational level.

At the present time, many of the regulatory approaches to security require OEMs to explicitly produce a structured Assurance Case of their product. This case can take many forms; though, it boils down to the following questions: What are your Claims, Arguments, and Evidence that you have assessed the cybersecurity risk of a vehicle and implemented sufficient cybersecurity controls and processes? What are you saying these controls and processes accomplish? How are you arguing the efficacy of those controls and processes? What evidence are you presenting to support that argument? Over time, the regulators will have seen a broader range of Assurance Cases to ask targeted specific questions about security controls and concepts – all of which requires a considered, well-documented approach to development.

Create a cross-brand cybersecurity task force

As an organization, the high-level objective should be to make cybersecurity everyone's responsibility. However, the subject matter expertise and cross domain specialisms that are necessary to understand the implications beyond a single component, the product, and all its ancillary processes is itself a specialist skill. Incentivize high-performers and respected SMEs from cybersecurity teams to join the taskforce.

While it can be helpful to communicate with customers, investors, and the general public through the language of brand, the reality is that the platforms themselves are more fundamental to the engineering process. This cross-brand cybersecurity task force should sit outside any brand structure that may exist and interface at a platform level.

Fill expertise gaps with trusted third-parties as appropriate

Security is a holistic discipline – motivated threat actors will always look for the path of least resistance when considering a target and attack methods. As automotive cybersecurity is a complex sub-discipline and the attack surface continues to grow as more connectivity and features are provided to fulfill customer demand, the amount and diversity of cybersecurity assurance work also grows. It's unlikely that an OEM has all the necessary skills and manpower to conduct all cybersecurity assurance activities completely in-house.

Establish relationships with trusted third-party assurance companies to fill technical gaps to support cybersecurity engineering, as well as testing of components, applications, and full vehicles as part of the assurance journey. These relationships can take many forms depending on the OEMs gaps and activity insourcing/outsourcing priorities. This will likely result in partnerships with multiple companies that align third-party strengths to OEM gaps.

Allow the task force to think creatively on how to improve cybersecurity assurance while working toward high-level goals

The new task force should have a wealth of technical talent combined with experience within the brands. Provide clear boundaries and goals but allow them the freedom to do what they do best – develop secure vehicle architectures and applications. Combining this expertise with proper technical program management will ensure

there are still appropriate checkpoints and milestones to check progress and realign approaches as necessary.

Example of high-level goals for the task force to further define and measure against:

- Manage automotive cybersecurity risk
- Ensure cybersecurity compliance across regions
- Minimize variants across regions (for components, applications, etc.)
- Maximize reuse of assurance processes and artifacts
- Minimize resources (e.g., funding and time)

Document the journey and continuously improve

Regular reviews of a product's security concept, during development and throughout the operational lifecycle is always recommended – to ensure that the identification of threats and the associated risk assessments remain accurate. However, ensuring that there is a documented process for potential security flaws for each component, system, etc. to be reported is one mechanism to ensure everyone is empowered to improve the organization's security.

Bringing it all together

Creating a framework for a group within the OEM that is accountable and responsible for *global* automotive cybersecurity would drive down cost while increasing assurance and compliance. This group can leverage the strengths of diverse, regional brands to build a cohesive, secure, and innovative security ecosystem that manages risk and ensures compliance while rationalizing spend. It is paramount to establish clear, shared objectives that align with both the collective goals of the organization and the specific aspirations of individual brands. This involves the creation of standardized yet flexible cybersecurity policies, processes, and tools that can be customized to meet the unique needs of each brand while ensuring a high level of security and efficiency across the board. These structures facilitate the exchange of ideas and best practices, driving technological advancements that benefit all brands while still allowing for individual expression and innovation.

We have outlined challenges of implementing these collaborative practices, from overcoming resistance to change, to managing resource allocation, to ensuring continuous engagement across all levels of the organization. We offer practical solutions and tools for navigating these challenges, including communication strategies, incentive systems, and metrics for measuring the success of collaborative efforts.

In conclusion, the paper provides a high-level roadmap for organizations looking to foster a culture of collaboration that enhances assurance, efficiency, safety, and innovation. By carefully balancing the needs and identities of different brands, companies can create a synergistic environment that not only drives progress in