STRATEGY ANALYTICS
Research, Experts, and Analytics

Infotainment and Telematics

Argus Helps Automakers Answer the Global Call for Automotive Cybersecurity Regulation

Automotive Multimedia and Communications (AMCS)

As vehicles become increasingly connected, their vulnerability to cyber-attacks increases. In the wake of multiple vehicle hacks, industry and government have recognized the critical need for cyber security to be integrated across the vehicle ecosystem and throughout the vehicle lifespan. However, the challenge of securing vehicles from intrusions is complex.
To support the automotive domain, industry and government bodies have independently published an array of principles, guidelines and proposed mandates that can be open to interpretation and present daunting challenges for automakers and the supply-chain.

Automotive

November 2018

Roger Lanctot
Tel: +1 617 614 0714
Email: rlanctot@strategyanalytics.com

Abstract

As vehicles become increasingly connected, their vulnerability to cyber-attacks increases. In the wake of multiple vehicle hacks, industry and government have recognized the critical need for cyber security to be integrated across the vehicle ecosystem and throughout the vehicle lifespan. However, the challenge of securing vehicles from intrusions is complex.

To support the automotive domain, industry and government bodies have independently published an array of principles, guidelines and proposed mandates that can be open to interpretation and present daunting challenges for automakers and the supply-chain.

Automakers can meet the various requirements and guidelines by aligning their vehicle cyber security strategies with the most comprehensive, mature, and widely adopted cyber security framework available, the US National Institute of Standards and Technology (NIST) Cybersecurity Framework. The framework, which is referenced by multiple automotive industry bodies, including the Alliance of Automobile Manufacturers, Association of Global Automakers, Auto-ISAC, National Highway Traffic Safety Administration (NHTSA), US Department of Transportation and Society of Automotive Engineers (SAE), provides an overarching cyber security strategy that includes five components:

- Identify
- Protect
- Detect
- Respond
- Recover

The NIST framework, developed for traditional IT security purposes, can be adapted to the automotive domain. Automakers can thereby develop the robust cyber security postures needed to meet the principles, guidelines and suggested mandates currently proposed in a way that aligns with the framework. Such solutions, taken together, will enable automakers to address specific sections of the published guidelines, principles and proposed mandates.

An example of one company doing this is Argus. This report provides an overview of Argus' solutions. Argus Cyber Security provides solutions and services that can to enable automakers to follow the NIST Cybersecurity Framework, minimize their exposure to cyber risk and detect malicious activity regardless of its origin or target within the vehicle. Argus products, including those for telematics and infotainment units, are designed to detect and respond in real time to cyber-attacks and software anomalies. Argus solution suites provide multi-level protection for enabling automakers to prepare for coming regulatory requirements and new standards setting activities.

For example, in September of 2017, the U.S. House of Representatives unanimously passed the SELF DRIVE Act (though it has yet to be passed by the U.S. Senate and signed into law by the U.S. President) which would require, among other things, the use of intrusion detection and prevention systems (IDPS) to safeguard key control systems like brakes and steering. Argus offers an IDPS solution that the company says offers near zero false positives and high detection rates.

Introduction

The growing threat of cyber-attacks on vehicles has launched a wave of standards-setting and regulatory activity across the globe intended to define a path forward to securing vehicles from hacks and intrusions. The need for action has been accented by the rapid increase in vehicle systems dependent on connectivity and the rapid evolution of automated driving.

The onset of embedded modems and other wireless connections in vehicles has thrust cyber security concerns to the forefront as regulators and the general public have been forced to confront their fears of rogue vehicles threatening the lives of drivers, passengers and pedestrians. As white-hat hackers such as Chris Valasek and Charlie Miller, formerly of IOActive, have demonstrated, the presence of telematics units in vehicles create new opportunities for the remote control of vehicles via wireless connections.

Moreover, digitization and connectivity in vehicles is generating large volumes of data, which has raised privacy concerns as sensitive driver information, such as driving routes, contacts and other private data, may present attractive targets for attack. The General Data Protection Regulation (GDPR), which serves to protect the privacy of EU citizens, requires OEMs to apply security measures to protect data from cyber-attacks.

Concern for automotive cyber security is not new — automakers have long been aware of the need to protect vehicles from hackers. Recently, with the advent of connected vehicles, multiple attack penetration points, including wireless access points (see Figure 2 later in this document), have been uncovered, tempting hobbyists, hacktivists, researchers and enthusiasts to manipulate vehicle software.

There have already been multiple high-profile vehicle hacks exposing serious threats, leading automakers and regulators to begin devoting serious attention and resources to mitigating the risks. Cyber security has become a necessity but implementation is a multi-faceted process that will take time, money and broad organizational change within each individual automaker.

Cyber security has become a necessity, but implementation is a multi-faceted process that will take time and money and broad organizational change within each individual automaker.

Further demonstrating the risks, many of the hacks in recent years have exploited basic flaws inherent in the design of vehicle software and hardware, as platforms and components from the IoT world are increasingly introduced into vehicles. Blueborne, Meltdown and Spectre are some recent examples of such vulnerabilities.

Automakers now see that threat vectors span everything from the vehicle design process to the supply chain and service bay at the dealership. Today, vehicle vulnerabilities even pose a threat to internal IT systems far removed from the vehicles themselves.

With hundreds of millions of connected vehicles expected on the road by 2020, regulators in the U.S. and Europe, standards-setting bodies and collaborative organizations, such as the recently created Auto-ISAC, have all recognized the public interest in this problem and published their own best practices for vehicle security — some of which call for immediate action by automakers and their suppliers. Other schemes propose heightening consumer awareness through vehicle security labels similar to that used on food packaging.

For several years, Argus has been confronting the challenge of securing vehicles from cyber-attacks. The company has developed a modular portfolio of solutions and services in order to provide automakers with the ability to create and maintain a strong cyber security posture. Argus' solutions can enable automakers to align their cyber security strategies with the U.S. National Institute of Standards and Technology's (NIST) Cybersecurity Framework, adapted for automotive cyber security: identify, protect, detect, respond and recover from cyber-attacks.[1] The automotive-adapted NIST components can be seen in Figure 1. The NIST Cybersecurity Framework provides a mature and comprehensive framework for helping businesses and organizations adopt a proactive approach towards cyber risk management and is already referenced in guidelines published by multiple automotive industry bodies including the Alliance of Automobile Manufacturers, Association of Global Automakers, Auto-ISAC, NHTSA and SAE.

Argus has developed a modular portfolio of solutions and services to help auto makers identify, protect, detect, respond and recover from attacks in accordance with the National Institute of Standards and Technology (NIST) cyber security framework.

Figure 1: Five continuous and concurrent cyber security components prescribed by NIST as they apply to vehicle cyber security

[1] National Institute of Standards and Technology. Cyber Security Framework https://www.nist.gov/cyberframework

Increased Vehicle Connectivity Comes with Increased Cyber Risk

Today, increasingly common vehicle components, applications and services reliant on wireless vehicle connections (e.g., cellular connectivity, digital radio, Wi-Fi and others) make us more entertained and productive than ever before, yet bring with them a host of vulnerabilities and risks. Even short-range communication for remote keyless systems and Bluetooth are sources of risk.

Further complicating vehicle security are legitimate aftermarket products enabling connected services such as usage-based insurance, diagnostic-based customer relationship management and, more recently, advanced safety technology. Increasingly, these systems seek access to vehicle inputs so they can constantly improve and enhance their context-based solutions. These mechanisms introduce a brand-new set of vulnerabilities.

Smartphone integration is also a critical issue since automakers are enabling in-vehicle pairing and tethering for drivers' devices, for example enabling the use of smartphone projection solutions. Such wired and wireless interfaces, though generally separated from on-board safety-critical systems, nevertheless add to the vehicle's attack surface, increasing the number of points through which a hacker could potentially insert malicious code into the vehicle.

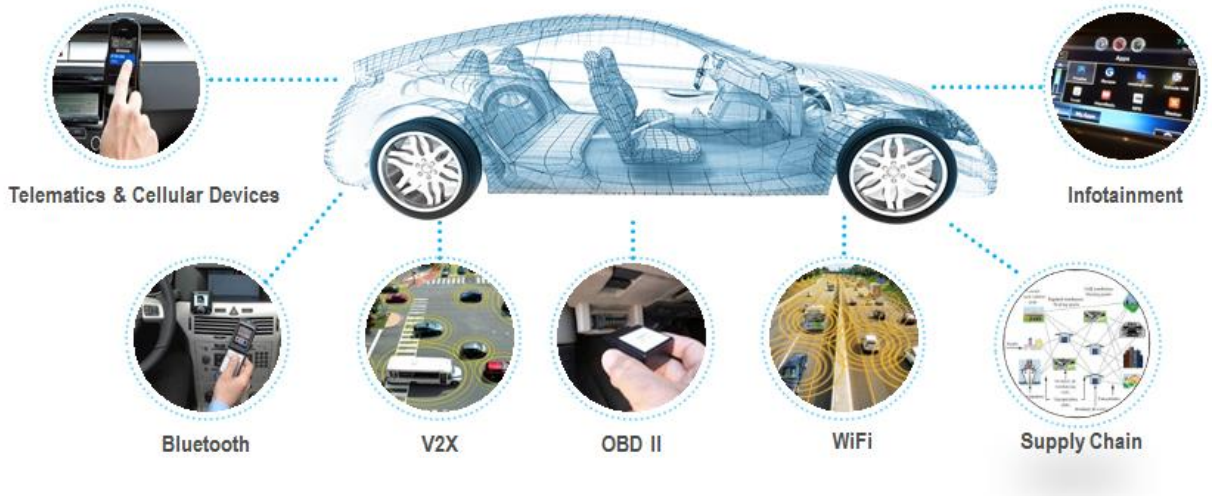

Figure 2: Connected vehicles provide multiple penetration points for cyber attacks

Argus Cyber Security has worked with aftermarket device suppliers like Zubie and Robert Bosch GmbH to identify and mitigate vulnerabilities in connected aftermarket platforms. In spite of those outreach efforts, and many others by Argus and other security companies, academics and white hat researchers, new attack vectors continue to emerge, requiring constant vigilance and the ability to respond.

Beyond the growing number of wireless connections built into the vehicles, the challenge of securing vehicles from intrusions is complicated by additional overarching factors, including, but not limited to:

- The long lifetime of a vehicle
- The extensive supply chain involved in producing vehicles
- The distributed software creation process, from development to validation and testing
- The distribution and service network supporting the maintenance of vehicles
- The integration of mobile devices with vehicles
- Rental and car-sharing scenarios in which the driver can be the threat actor
- The increasing availability of 3rd party aftermarket connectivity solutions
- The increasing number of connected services that enable remote control of in-vehicle functions

With this ever increasing number of attack surfaces in vehicles, and governments and industry bodies looking at vehicle cyber security more closely, Argus offers solutions that align with a broad range of guidelines, standards, and potential legislation.

Compliance with Guidelines, Standards and Potential Mandates

Vehicle cyber security is a holistic exercise that includes the entire vehicle value chain — OEMs, suppliers, the design and production process, fleet managers and more. Some of the principles, guidelines and proposed mandates Argus believes the auto industry should prepare for include:

- Regulations
  - SELF DRIVE Act[2]
  - AV START Act[3]
  - General Data Protection Regulation (GDPR)[4]
- Guidelines
  - U.S. Senate Bipartisan Principles for Automotive Cybersecurity[5]
  - U.K. Principles for Self-Driving Vehicles[6]
  - NHTSA (National Highway Traffic Safety Administration) Cybersecurity Best Practices[7]
  - U.S. Department of Transportation – Preparing for the Future of Transportation: Automated Vehicles 3.0[8]
  - NHTSA – A Vision for Safety for Automated Driving Systems[9]
  - Auto-ISAC Automotive CyberSecurity Best Practices[10]
  - ACEA Principles of Automobile Cybersecurity[11]
  - ENISA Cyber Security and Resilience of Smart Cars[12]
  - NIST Framework for Improving Critical Infrastructure Cybersecurity[13]
  - Alliance of Automobile Manufacturers and Association of Global Automakers Framework for Automotive Cybersecurity Best Practices

These documents, and others, call for comprehensive automotive cyber security methodologies and solutions, requiring know-how that automakers have not traditionally focused on. In addition to some of the national regulations and guidelines listed above, strict international standards and regulations currently being developed by joint SAE/ISO working groups (i.e., ISO/SAE 21434 Automotive Cybersecurity Standard) and the United Nations Economic Commission for Europe (e.g., UNECE task force on cyber security and over-the-air software updates) promise only to increase the required level of security as automakers build more and more networked solutions into future vehicles.

---

[2] SELF DRIVE Act
[3] AV START Act
[4] General Data Protection Regulation
[5] Bipartisan Principles for Self-Driving Vehicles Legislation
[6] The key principles of vehicle cyber security for connected and automated vehicles
[7] NHTSA Cyber Security Best Practices for Modern Vehicles
[8] U.S. Department of Transportation – Preparing for the Future of Transportation: Automated Vehicles 3.0
[9] NHTSA A Vision for Safety for Automated Driving Systems
[10] Auto ISAC Automotive Cybersecurity Best Practices
[11] ACEA Principles of Automobile Cybersecurity
[12] ENISA Cyber Security and Resilience of Smart Cars
[13] NIST Framework for Improving Critical Infrastructure Cybersecurity

Although automotive cyber security will be an ongoing challenge for the automakers, collaborating with companies with specialized knowledge of both the auto industry and cyber security will allow vehicle manufacturers and fleets to benefit from the opportunities of connectivity while minimizing the risks. In Table 1 below, some of the security controls available to the industry can be seen divided up according to the components of the NIST Framework. Also in Table 1, the specific Argus solution suite that addresses each NIST component can also be seen.

Table 1: Examples of suggested security controls per NIST component

NIST Component	Identify	Protect	Detect	Respond	Recover
Available Security Controls	• Threat assessments • Risk analysis • Vulnerability analysis • Penetration testing • Design review • Code review • Cyber security consulting and management services	• ECU Hardening • Secure on-board communications • Firewalls and In-vehicle intrusion protection (IPS) • Policy based behavioural enforcement • Secure boot and authenticated execution • Cryptography • Security Tokens • CFI	• In-vehicle network detection systems • in-vehicle host-based detection systems • Cross-fleet back-end analysis and investigation • Detailed alerts	• Autonomous in-vehicle response • Security Operation Center to enable: • Forensic tools • Security Updates Over- the-Air • Services • Incident response	• Software Updates Over-The-Air Solution
Argus Solutions					

Argus trusted advisers identify security gaps in fleets, vehicles and components.

Argus In-Vehicle Protection prevents, detects and responds in real time to attacks on the in-vehicle network.

Argus Lifespan Protection protects vehicles throughout their lifetime with ongoing monitoring, cross-fleet big data analysis, incidence response tools & more.

Argus Connectivity Protection prevents, detects and responds in real time to attacks on infotainment, telematics units and other connected ECUs.

Argus ECU Protection is designed to provide a last layer of defense to protect critical ECUs from attacks and protects the vehicle from ECUs compromised in the supply chain.

Software Updates Over-the-Air enable OEMs and fleet managers to respond and recover from attacks in minimal time and customer inconvenience.

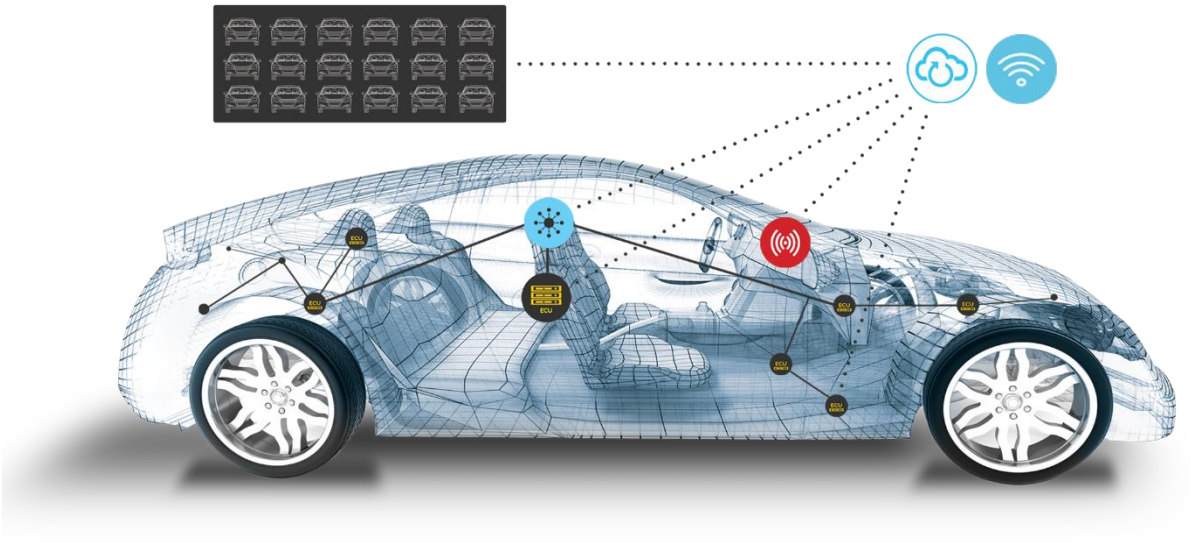

Figure 3: Argus Solution Suites in the Vehicle

If automakers and connected fleets address each component of the NIST Framework, industry standards and regulations can be met. To illustrate this point, Table 2 divides specific clauses from the guidelines and proposed mandates according to the NIST components.

Table 2: The Principles, Guidelines and Proposed Mandates According to NIST Component and Region

Note: *Each of the sections specified in this table is detailed in full in the next segment of this paper.*

Identify	Protect	Detect	Respond	Recover
US Senate Bipartisan Principles for Automotive Cyber Security • Cybersecurity…must be an integral feature of self-driving vehicles from the very beginning of their development. • Legislation must address the connectivity of self-driving vehicles and potential cyber security vulnerabilities before they compromise safety. **AV START Act** • Sec. 14. (b) (1), (b) (2) (D) - (b) (2) (G) **SELF DRIVE Act** • Sec. 5. (a) (1) (A), (a) (3) • Sec. 9. (e) (3) **NHTSA Cybersecurity Best Practices** • Sec. 5.1-5.2 • Sec. 6.1-.6.6, 6.6.1 - 6.6.3, 6.7.1-6.6.7	**AV START Act** • Sec. 14. (b) (2) (A) **SELF DRIVE Act** • Sec. 5. (a) (1) (B), (a) (3) **NHTSA Cybersecurity Best Practices** • Sec. 5.1 - 5.2 • Sec. 6.6.1 - 6.6.2 • Sec. 6.7.3 - 6.7.5, 6.7.8 - 6.7.11 **Auto ISAC Automotive Cybersecurity Best Practices** • Sec. 3.0 • Sec. 4.3, 4.4 **U.S. Department of Transportation – Preparing for the Future of Transportation: Automated Vehicles 3.0** • ROLES IN AUTOMATION: PRIVATE	**AV START Act** • Sec. 14. (b) (2) (B) **SELF DRIVE Act** • Sec. 5. (a) (1) (B), (a) (3) **NHTSA Cybersecurity Best Practices** • Sec. 5.1 - 5.2 • Sec. 6.6.1 - 6.6.2 **Auto ISAC Automotive Cybersecurity Best Practices** • Sec. 3.0 • Sec. 4.3, 4.4 **U.S. Department of Transportation – Preparing for the Future of Transportation: Automated Vehicles 3.0** • ROLES IN AUTOMATION: PRIVATE	**AV START Act** • Sec. 14. (b) (2) (B) - (b) (2) (C) **SELF DRIVE Act** • Sec. 5. (a) (1) (A) - (a) (1) (B), (a) (3) **NHTSA Cybersecurity Best Practices** • Sec. 5.1 - 5.2 • Sec. 6.6.1 - 6.62 • Sec. 6.7.4 - 6.7.5, 6.7.9, 6.7.11 **NHTSA Automated Driving Systems: A Vision for Safety** • **Sec. 1 (7) Vehicle Cybersecurity** • Page 11: Follow robust cyber incident response plans. **Auto ISAC Automotive Cybersecurity Best Practices** • Section 3.0 • Sec. 4.3 - 4.5 **U.S. Department of**	**AV START Act** • Sec. 14. (b) (2) (D) **SELF DRIVE Act** • Sec. 5. (a) (1) (A) **NHTSA Cybersecurity Best Practices** • Sec. 5.1 - 5.2 • Sec. 6.6.1-6.6.3 **Auto ISAC Automotive Cybersecurity Best Practices** • Sec. 4.5 • Sec. 4.7 **SAE J3061** • Sec. 5.6

Identify	Protect	Detect	Respond	Recover
NHTSA Automated Driving Systems: A Vision for Safety • Sec. 1 (7) Vehicle Cybersecurity • Page 11 – minimize risk during design **Auto ISAC Automotive Cybersecurity Best Practices** • Sec. 3.0, 4.1-4.3, 4.6-4.7 U.S. Department of Transportation **U.S. Department of Transportation – Preparing for the Future of Transportation: Automated Vehicles 3.0** • Roles in Automation: Private			**Transportation – Preparing for the Future of Transportation: Automated Vehicles 3.0** • Roles in Automation: Private	

European Commission Proposal for a Regulation of the European Parliament and of the Council on ENISA, the "EU Cybersecurity Agency": The proposal explains how cybersecurity certification including product labels will, "…. make ICT (information and communication technology)-based systems, including connected objects [such as vehicles], more cyber-secure."

Identify	Protect	Detect	Respond	Recover
ACEA Principles of Automobile Cybersecurity	**ACEA Principles of Automobile Cybersecurity**	**ACEA Principles of Automobile Cybersecurity**	**ACEA Principles of Automobile Cybersecurity**	**ACEA Principles of Automobile Cybersecurity**

Identify	Protect	Detect	Respond	Recover
• Principle 1 - 3, 5 **ENISA Cyber Security and Resilience of Smart Cars** • GP-PS-01, 03 • GP-OM-01-06, • GP-OM-008 • GP-SF-07-10, 18-19, 22-24, 27 • Section 5 Recommendations **GDPR** • Chapter 4, Section 1 - Article 24 (1), (2), Article 25, Article 28 (1) • Chapter 4, Section 2 - Article 32 (1) a, b, c, d • Chapter 4, Section 3 - Article 35 1, 7, 11	• Principle 2 **ENISA Cyber Security and Resilience of Smart Cars** • GP-OM-10 • GP-SF-04, 06, 16, 20, 22-27 **GDPR** • Chapter 2, Article 5 1 (f) • Chapter 4, Section 1 - Article 24 (1), (2), Article 25 Chapter 4, Section 2 - Article 32 (1) a, b, c	• Principle 2 **ENISA Cyber Security and Resilience of Smart Cars** • GP-OM-06 • GP-SF-01, 26 **GDPR** • Chapter 4, Section 1 - Article 24 (1), (2), Article 25 Chapter 4, Section 2 - Article 32 (1) b, d	• Principle 2 • Principle 4 • Principle 5 **ENISA Cyber Security and Resilience of Smart Cars** • GP-OM-06 - 07 • GP-OM-07 • GP-SF-01, 04, 06, 18, 20, 24-27 **GDPR** • Chapter 4, Section 2 - Article 32 (1) b, c, d	• Principle 2 • Principle 4 • Principle 5 **ENISA Cyber Security and Resilience of Smart Cars** • GP-OM-06, 07, 10 • GP-OM-07 • GP-OM-10 • GP-SF-06, 16, 18, 20, 25, 26 • GP-SF-16, 17, 18, 20, 25,26 **GDPR** • Chapter 4, Section 2 - Article 32 (1) b, c, d • Chapter 4, Section 3 - Article 35 (11)

Identify	Protect	Detect	Respond	Recover
The Key Principles of Vehicle Cyber Security for Connected and Automated Vehicles • Principles 2, 2.3, 3.1-3.3, 4.2, 5.1, 6.4	**The Key Principles of Vehicle Cyber Security for Connected and Automated Vehicles** • Principle 3.3-3.4, 5.1, 7, 8.1	**The Key Principles of Vehicle Cyber Security for Connected and Automated Vehicles** • Principle 3.3-3.4, 5.1, 7, 8.1	**The Key Principles of Vehicle Cyber Security for Connected and Automated Vehicles** • Principle 2, 2.3, 3-3.4, 5.1, 6, 8.1-2	**The Key Principles of Vehicle Cyber Security for Connected and Automated Vehicles** • Principle 6 ○ Principle 6.2 Principle 6.3

Identify	Protect	Detect	Respond	Recover
●				
In 2015, the Japanese government issued a cybersecurity strategy paper stating its intention to, “establish comprehensive guidelines and standards for IoT security…. including automotive.” Advisors to the government of Japan are consulting with foreign companies and institutions. In addition, JasPar, a Japanese auto industry alliance for the promotion of vehicle electronics standardization, has established a cyber security promotion work group.				

A Detailed Look into the Relevant Principles, Guidelines and Proposed Mandates

1. **U.S. Senate Bipartisan Principles for Automotive Cybersecurity**
   - Cybersecurity should be a top priority for manufacturers of self-driving vehicles and it must be an integral feature of self-driving vehicles from the very beginning of their development."
   - "Legislation must address the connectivity of self-driving vehicles and potential cybersecurity vulnerabilities before they compromise safety."

2. **SELF DRIVE Act** or Safely Ensuring Lives Future Deployment and Research In Vehicle Evolution Act

   - **Section 5. (a)(1)(A)**: "A process for identifying, assessing and mitigating reasonably foreseeable vulnerabilities from cyber-attacks or unauthorized intrusions, including false and spurious messages and malicious vehicle control commands;"
   - **Section 5. (a)(1)(B)**: "A process for taking preventive and corrective action to mitigate against vulnerabilities in a highly automated vehicle or a vehicle that performs partial driving automation, including incident response plans, intrusion detection and prevention systems that safeguard key controls, systems, and procedures through testing or monitoring, and updates to such process based on changed circumstances."
   - **Section 5. (a)(3)**: "A process for limiting access to automated driving systems."
   - **Section 9. (e)(3)**: "Cybersecurity for the testing, deployment, and updating of automated driving systems with respect to supply chain risk management, interactions with Information Sharing and Analysis Centers and Information Sharing and Analysis Organizations, and a framework for identifying and implementing recalls of motor vehicles or motor vehicle equipment;"

3. **AV START Act –** The American Vision for Safer Transportation through Advancement of Revolutionary Technologies Act

   - **Section 14. (b)(1)**: "In general—each manufacturer of a highly automated vehicle or automated driving system shall develop, maintain, and execute a written plan for identifying and reducing cybersecurity risks to the motor vehicle safety of such vehicles and systems."
   - **Section 14. (b)(2)**: "The plan…shall include a process for –
     - (A) the risk-based prioritized identification and protection of safety-critical vehicle control systems and the broader transportation ecosystem, as applicable;
     - (B) the efficient detection and response to potential vehicle cybersecurity incidents in the field;
     - (C) facilitating expeditious recovery from incidents as they occur;
     - ''(D) the institutionalization of methods for the accelerated adoption of lessons learned across industry through voluntary exchange of information pertaining to cybersecurity incidents, threats, and vulnerabilities, including the consideration of a coordinated cybersecurity vulnerability disclosure policy or other related practices for collaboration with third-party cybersecurity researchers;
     - (E) the identification of the point of contact of the manufacturer with responsibility for the management of cybersecurity;

- (F) the use of segmentation and isolation techniques in vehicle architecture design, as appropriate;"

4. **NHTSA Cybersecurity Best Practices for Modern Vehicles (BP)**
   - **Section 5.1** Layered Approach
     - "A layered approach to vehicle cybersecurity reduces the probability of an attack's success and mitigates the ramifications of a potential unauthorized access."
     - "This approach should:
       - Be built upon risk-based prioritized identification and protection of safety-critical vehicle control systems and personally identifiable information;
       - Provide for timely detection and rapid response to potential vehicle cybersecurity incidents in the field;
       - Design-in methods and measures to facilitate rapid recovery from incidents when they occur;"
   - **Section 5.2** Information Technology Security Controls
     - "NHTSA recommends that the automotive industry review and consider the information technology (IT) security suite of industry standards…to improve the cybersecurity of IT infrastructures for the vehicle controller development, dealer and service environments, and the supply-chain as they are applicable."
   - **Section 6.1** Vehicle Development Process with Explicit Cybersecurity Considerations
     - "The automotive industry should follow a robust product development process…Companies should make cybersecurity a priority by using a systematic and ongoing process to evaluate risks…through the entire life-cycle of the vehicle. The life-cycle of a vehicle includes conception, design, manufacture, sale, use, maintenance, resale, and decommissioning. Safety of vehicle occupants and other road users should be of primary consideration when assessing risks."
   - **Section 6.2** Leadership Priority on Product Cybersecurity
     - "…NHTSA recommends that companies developing or integrating safety critical vehicle systems prioritize vehicle cybersecurity and demonstrate management commitment to doing so…"
   - **Section 6.4** Vulnerability Reporting / Disclosure Policy
   - **Section 6.5** Vulnerability / Exploit / Incident Response Process
   - **Section 6.6** Self-Auditing
   - **Section 6.7** Fundamental Vehicle Cybersecurity Protections
     - **Section 6.7.7**: "Use segmentation and isolation techniques in vehicle architecture."
     - **Section 6.7.8**: "Critical safety messages…should employ a message authentication scheme to limit the possibility of message spoofing."
     - **Section 6.7.9**: **"**An immutable log of events sufficient to reveal the nature of a cybersecurity attack…should be maintained."
     - **Section 6.7.11**: "...design-in features that could allow for changes in network routing rules to be quickly propagated and applied to one, a subset, or all vehicles."

5. **NHTSA Automated Driving Systems, A Vision for Safety**
   - **Section 1 (7)**: "Entities are encouraged to follow a robust product development process based on a systems engineering approach to minimize risks to safety, including those due to cybersecurity threats and vulnerabilities."

- **Section 1 (7)**: "This process should include a systematic and ongoing safety risk assessment for each ADS, "the overall vehicle design into which it is being integrated, and when applicable, the broader transportation ecosystem."
- **Section 1 (7)**: "Entities are encouraged to design their ADSs following established best practices for cyber vehicle physical systems."
- **Section 1 (7)**: "Entities are further encouraged to establish robust cyber incident response plans and employ a systems engineering approach that considers vehicle cybersecurity in the design process. Entities involved with ADSs should also consider adopting a coordinated vulnerability reporting/disclosure policy.
- **Section 1 (7)**: **"**Entities are encouraged to consider and incorporate voluntary guidance, best practices, and design principles published by National Institute of Standards and Technology (NIST21), NHTSA, SAE International, the Alliance of Automobile Manufacturers, the Association of Global Automakers, the Automotive Information Sharing and Analysis Center (Auto-ISAC),22 and other relevant organizations, as appropriate"

6. **U.S. Department of Transportation – Preparing for the Future of Transportation: Automated Vehicles 3.0**

"It is the responsibility of ADS developers, vehicle manufacturers, parts suppliers... to follow best practices, and industry standards, for managing cyber risks in the design, integration, testing, and deployment of ADS."

- **ROLES IN AUTOMATION: PRIVATE**:
  - To mitigate potential threats, [automakers]...should include strong security and functional testing of...technology, people, and processes…
  - [In everything from] limited to full ADS deployment, [automakers must address cybersecurity]...in a production manner.
  - Key decision makers should have an effective and flexible security program in place...
  - Plans to respond to cyber-attacks should be exercised, and should be aligned with emergency management and recovery protocols…

7. **NIST Framework for Improving Critical Infrastructure Cybersecurity**

- The Framework, developed in collaboration with industry, provides guidance to an organization on managing cybersecurity risk. The Framework **for Improving Critical Infrastructure Cybersecurity** is frequently referenced in Auto-ISAC Best Practices and NHTSA calling for automakers to apply the framework to vehicle cyber security
- **NIST:** "2.1: The Framework Core consists of five concurrent and continuous Functions—Identify, Protect, Detect, Respond, Recover. When considered together, these Functions provide a high-level, strategic view of the lifecycle of an organization's management of cybersecurity risk."
- **NIST:** "Identify - Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities."
- **NIST:** "Protect - Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services."
- **NIST:** "Detect – Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event."
- **NIST:** "Respond - Develop and implement the appropriate activities to take action regarding a detected cybersecurity event."
- **NIST:** "Recover – Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event."

8. **Auto ISAC Automotive Cybersecurity Best Practices –** Auto-ISAC, formed by car makers at the request of regulators, has published its own set of best practices. The Best Practices expand on the Framework for Automotive Cybersecurity Best Practices ("Framework") published in January 2016 by the Alliance of Automobile Manufacturers ("Auto Alliance") and the Association of Global Automakers ("Global Automakers").

- **Section 3.0**: "The Best Practices include 7 functions:
    - Security by design
    - Risk assessment and management
    - Threat detection and protection
    - Incident response (available to industry stakeholders)
    - Collaboration and engagement with appropriate third parties (available to industry stakeholders)
    - Governance (in progress); awareness and training
- **Section 4**: Best Practices Overview
- "Effective governance aligns a vehicle cybersecurity program with an organization's broader mission and objectives."
- **Section 4.2**: "Risk assessment and management strategies mitigate the potential impact of cybersecurity vulnerabilities. Best Practices focus on processes for identifying, categorizing, prioritizing, and treating cybersecurity risks that could lead to safety and data security issues."
- **Section 4.3**: "Secure vehicle design involves the integration of hardware and software cybersecurity features during the product development process."
- **Section 4.4**: "Threat Detection and Prevention: Proactive cybersecurity through the detection of threats, vulnerabilities, and incidents…"
- **Section 4.5**: "Incident Response and Recovery: … processes to inform a response to cybersecurity incidents affecting the motor vehicle ecosystem. Best Practices include protocols for recovering from cybersecurity incidents in a reliable and expeditious manner, and ways to ensure continuous process improvement."
- **Section 4.6**: "Training and awareness programs help cultivate a culture of security and enforce vehicle cybersecurity responsibilities."
- **Section 4.7**: "Collaboration and Engagement with Appropriate Third Parties… When faced with cybersecurity challenges, the industry is committed to engaging with third parties, including peer organizations, suppliers, cybersecurity researchers, government agencies and Auto-ISAC, as appropriate."
-

9. **SAE J3061**

This recommended practice establishes a set of high-level guiding principles for cybersecurity as it relates to automotive cyber-physical systems to be utilized in series production.

- Section 5.1: "Conduct the appropriate threat analysis and risk assessment."
- Section 5.2: "Apply 'Defense in Depth', particularly for the highest risk threats. This means that threat mitigation should not rely on only a single Cybersecurity Control…"
- Section 5.4: "Implement cybersecurity in concept and design phases."
- Section 5.5.: "Implement cybersecurity in development & validation."
- Section 5.6: "Implement cybersecurity in incident response."
- Section 5.7: "

Understand key cybersecurity principles

- Protect Personally identifiable information (PII) and Sensitive data.
- Use the principle of "Least Privilege" – All components run with the fewest possible permissions.
- Apply "Defense in Depth", particularly for the highest risk threats.
- Prohibit risky changes to calibrations and/or software.
- Vehicle-Level: Prevent users from making unauthorized changes that could reduce security for the vehicle after it has been sold. Some potential violations of this principle include:
    - "Tuners", Software that may come from a DVD, Bluetooth-paired phone, etc.

Implement cybersecurity in concept and design phases

- The system should be defined with cybersecurity in mind, starting in the concept phase of the development lifecycle.
- Analyze threats (i.e., initiated external or internal to the system, and often of malicious intent) to determine what risks and attack surfaces will be faced by the system.
- Implement cybersecurity analysis and management tools that enable engineers to determine and configure the optimal security level for the system.

Implement cybersecurity in development and validation

- Review design to assess whether the cybersecurity requirements are being met.
- Conduct testing to confirm that the requirements that were established for cybersecurity at the beginning of the design phase have been met in the modules/controllers/ECUs and in the overall vehicle design.
- Test software patch/revision deployment tools and processes to ensure that any approved re-flashes to the vehicle software can be done without adversely affecting the vehicle's cybersecurity defenses.

Implement cybersecurity in incident response

- Revise (or create) the Incident Response Process so that it comprehends cybersecurity incidents.
- Publish deployment guides.
- Determine how software and/or calibration updates will be made if there is an incident.
- Vehicle-Level: Develop appropriate material for dealerships, customer assistance help lines, websites, and owner's manuals.

1. The **European Automobile Manufacturers Association (ACEA)**, representing Europe's car, van, truck and bus manufacturers, has published its own Principles of Automobile Cybersecurity, identifying a set of six key principles to enhance the protection of connected and automated vehicles against cyber threats.[14]

    - **ACEA Principle 1**: Cultivating a cybersecurity culture – "Vehicle manufacturers recognize that addressing cybersecurity issues requires a very accurate skill set when dealing with risk management, secure design, training and awareness, and penetration testing. In-house resources may…be supported by trusted outsourced security specialists when…additional skills [are required]."
    - **ACEA Principle 2**: Adopting a cybersecurity life cycle for vehicle development – "ACEA believes that addressing critical cybersecurity issues is crucial and should be a fully integrated part of the vehicle development process."

[14] ACEA Principles of Automobile Cybersecurity

- **ACEA Principle 3**: Assessing security functions with testing phases – "Testing should be performed by qualified testers who have not been part of the development phase. Penetration testing can be employed for high-risk parts."
- **ACEA Principle 4**: Managing a security update policy – "As cyber threats evolve, so must the methods by which they are tackled and countered by a vehicle's cyber security system. These systems will therefore be updated when needed."
- **ACEA Principle 5**: Providing incident response and recovery – "Incident response plans are set up. They document processes to form a response to cybersecurity incidents affecting the vehicle. These plans document the incident response, from its identification and, where applicable, its containment through remediation and recovery."

2. ENISA Cyber Security and Resilience of Smart Cars, Good Practices and Recommendations

"The objective of this study is to identify the good practices to ensure the security of smart cars against cyber threats, with the particularity that Smart Cars security shall also guarantee safety."

- **Section 4.3.1 – Policy and Standards**
  - **GP-PS-01 – Adherence to regulation.** "Industry actors shall, as a first step, adhere to regulation related to security and privacy."
  - **GP-PS-03 – Traceability.** "Car manufacturers and Tier actors shall ensure that appropriate technical measures (e.g. logging, distinct authentication, transparency provided through OEM/Tier sites concerning each particular car/component, integration with Type Approval authorities and monitoring agencies) exist allowing for tracing liability between actors."
- **Section 4.3.2 – Organizational Measures – General**
  - **GP-OM-01 - Designate a dedicated security team. "**Actors of the smart car industry should rely on specialists, notably for secure design, penetration testing and risk management…"
  - **GP-OM-02 - Define a dedicated Information Security Management System (ISMS). "**Actors of the smart car industry should define an ISMS, possibly inspired from SAE J3061, ISO 27001 or NIST 800-53, and refine it to address the specific needs of their industry, notably the management of Tier-1 and Tier-2 actors, and processes to ensure continuous isolation of the components from aftermarket products."
- **Organizational Measures – Secure Development**
  - **GP-OM-03 - Assess the threat model and use cases. "**Actors of the smart car industry should perform a threat analysis prior to development possibly inspired from SAE-J3061 TARA approach (including EVITA, TVRA, OCTAVE and HEAVENS methods) or possible from the risk management approach of ISO 31000. Efforts in this direction are also done in the context of ISO AWI 21434."
  - **GP-OM-04 - Provide security and privacy by design.** Actors of the smart car industry should plan their development lifecycles to ensure that security and privacy are taken into account no later than the design phase, in order to address the threats identified in the risk assessment.
  - **GP-OM-05 - Implement and test the security functions. "**Actors of the smart car industry should clearly define appropriate security functions that will be explicitly implemented and tested during the development lifecycle..."
- **Organizational Measures – Security Until the End-of-Life**
  - **GP-OM-06 - Assess the security controls and patch vulnerabilities. "**Actors of the smart car industry should define appropriate assessment procedures to regularly check the effectiveness of their security functions, and patch them whenever needed."

- **GP-OM-07 - Define a security update policy. "**Actors of the smart car industry should define an update policy for security patches…OTA update mechanisms whenever possible..."
- **GP-OM-08 - Perform a vulnerability survey. "**Actors of the smart car industry should perform a vulnerability survey to be proactively able to fix security issues before they can be used in the wild..."
- **GP-OM-09 - Check the security assumptions regularly during life-time. "**The devices and services made assumptions to ensure that the security requirements are sufficient (limitations in the usage of the vehicle, assumed properties of the environment, assumed properties of cryptographic properties…)…"
- **GP-OM-10 - Protect the software update mechanism. "**Vendors should protect the updates (typically via encryption and digital signature) and protect the application of an update on the device. Eventually, the update server and infrastructure (including diagnostic tools) should also be protected."
- **GP-OM-11 - Raise user awareness. "**Vendors and public authorities should explain users what actions can contribute to mitigate potential threats, especially how to securely use interfaced systems such as a smartphone…"

- **Section 4.3.3 – Technical – Security Functions – Security Audit**
  - **GP-SF-01 - Security events must be securely logged.** "Access to the logs must be documented and protected from disclosure to unauthorized users…"
- **Security Functions – Communication Protection**
  - **GP-SF-03 - Provide end-to-end protection in confidentiality and integrity,** "Using protocols that resist to replay attacks. Favour methods providing forward secrecy whenever possible, for WAN traffic (internet, mobile network) as well as local networks."
  - **GP-SF-04 - Mitigate vulnerabilities or limitations of standard security library.** "Developers must be aware of the vulnerabilities and limitations of the third-party components they use. They should mitigate them whenever possible by patching and by securing the configuration of the communication stacks…"
  - **GP-SF-05 - Consider denial of service as a usual threat to communication infrastructures.**
  - **GP-SF-06 - Protect remote monitoring and administration interfaces. "**Vendors should protect all monitoring and administration interfaces by mutual authentication and access control mechanisms."
- **Security Functions – Cryptography**
  - **GP-SF-07 - Do not create proprietary cryptographic schemes, but use state-of-the-art standards instead.** "If needed, consider getting advice from security experts or your national cybersecurity agency…Additionally, consider the expected life duration of the vehicle and find advice on the relevant key size…"
  - **GP-SF-08 - Rely on an expert in cryptography**, "…code review should be performed to ensure that HW or a standard implementation of cryptography is properly used. The code review would ideally be performed by a third party…"
  - **GP-SF-09 - Consider using dedicated, and independently audited, hardware security modules.**
  - **GP-SF-10 - Cryptographic keys should be securely managed**.
- **Security Functions – Identification, Authentication, Authorization**
  - **GP-SF-16 - Use mutual authentication for remote communication.** "Devices or users connecting to a server must be able to authenticate the server. Reciprocally, servers must be able to authenticate clients and users."
  - **GP-SF-18 - Implement access control measures to separate the privileges of different users and the privileges of different applications as well as to ensure traceability of access and**

modifications. "…OEMs and Tier Actors shall employ a sufficient and flexible infrastructure for "distinct" cryptographic keys per Tier Actors, garage personnel or vehicle owner."

- **GP-SF-20 - Enforce session management policies to avoid session hijacking.**

- **Security Functions – Self-Protection**
  - **GP-SF-22 - Define a consistent policy for self-protection.** "Vendors should challenge every security function of their design, consider how they could be bypassed or weakened, and eventually implement self-protection measures."
  - **GP-SF-23 – Implement Hardware self-protection. "**Vendors should define measures to protect hardware against physical attacks or observation…"
  - **GP-SF-24 – Implement Software self-protection.** "Vendors should define measures to protect existing security functions, typically by validating inputs and outputs, or by separating the capacities of the different software components..."
  - **GP-SF-25 – Protect Non-user data.** "Vendors should protect data enforcing the security functions..."
  - **GP-SF-26 – Perform Hardening. Vendors should actively reduce the attack surface of the product or device.** "This includes…providing secure configuration by default, as well as integrating malware protection. Some actors may consider intrusion detection systems for internal subnetworks (for example CAN bus monitoring) …"
  - **GP-SF-27 – Isolate components**. "Vendors should reduce the capacity for attackers to jump from a component to another, either by a physical disconnection or by using gateways."

3. **European Commission Proposal for a regulation of the European Parliament and of the Council on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology Cybersecurity Certification ("Cybersecurity Act")**
   - "[ENISA] to help put in place and implement the EU-wide certification framework…to ensure that [information communication technology] products and services, [such as connected vehicles], are cyber secure." Intended to give end users understanding of level of product security (like food labels).

4. **General Data Protection Regulation** (GDPR)
   - **Chapter 2, Article 5 1 (f)** - [Personal data shall be] processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').
   - **Chapter 2, Article 33 (1)** - In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55
   - **Chapter 4, Section 1, Article 24 (1)** - Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary.
   - **Chapter 4, Section 1, Article 24 (2)** - Where proportionate in relation to processing activities, the measures referred to in paragraph 1 shall include the implementation of appropriate data protection policies by the controller.
   - **Chapter 4, Section 1, Article 25** - Data protection by design and by default.
   - **Chapter 4, Section 1, Article 28** - Where processing is to be carried out on behalf of a controller, the controller shall use only processors providing sufficient guarantees to implement appropriate technical and

organisational measures in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject.

- **Chapter 4, Section 2, Article 32 (1)** - "...the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate."
    - **a** - the pseudonymisation and encryption of personal data.
    - **b** - the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services.
    - **c** - the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident.
    - **d** - a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.
- **Chapter 4, Section 3, Article 35** - Data protection impact assessment.
    - **1** - Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data…
    - **7** - The assessment shall contain…
    - **11** - Where necessary, the controller shall carry out a review to assess if processing is performed in accordance with the data protection impact assessment at least when there is a change of the risk represented by processing operations.

1. **The Key Principles of Vehicle Cyber Security for Connected and Automated Vehicles –** The Department for Transport, in conjunction with Centre for the Protection of National Infrastructure (CPNI), created the following key principles:
   - **Principle 1**: "Personal accountability of board members" of companies creating self-driving vehicles for cybersecurity."
   - **Principle 2**: "Security risks are assessed and managed appropriately and proportionately."
   - **Principle 2.3**: "Security risk assessment and management procedures are in place within the organization. Appropriate processes for identification, categorization, prioritization and treatment of security risks, including those from cyber, are developed.
   - **Principles 3, 3.1, 3.2**: "Organizations apply product aftercare and incident response to ensure lifetime security. Organizations plan for how to maintain security over the lifetime of their systems, including any necessary aftersales support services. Organizations respond to potential compromises of safety critical assets, non-safety critical assets and system malfunctions."
   - **Principle 3.3**: "There is an active program in place to identify critical vulnerabilities and appropriate systems in place to mitigate them in a proportionate manner."
   - **Principle 3.4**: "Organizations ensure their systems are able to support data forensics and the recovery of forensically robust, uniquely identifiable data. This may be used to identify the cause of any cyber, or other, incident."
   - **Principles 5, 5.1, 5.2**: "Systems are designed using a defense-in-depth approach. The security of the system does not rely on single points of failure, security by obscuration or anything which cannot be readily changed, should it be compromised. The security architecture applies defense-in-depth and segmented techniques, seeking to mitigate risks with complementary controls such as monitoring, alerting, segregation, reducing attack surfaces (such as open internet ports), trust layers/ boundaries and other security protocols."
   - **Principles 6, 6.2, 6.3, 6.4**: "The security of all software is managed throughout its lifetime. It must be possible to ascertain the status of all software, firmware and their configuration, including the version, revision and configuration data of all software components. It's possible to safely and securely update software and return it to a known good state if it becomes corrupt. Software adopts open design practices and peer reviewed code is used where possible. Source code is able to be shared where appropriate."
   - **Principle 8.1**: **"**The system must be able to withstand receiving corrupt, invalid or malicious data or commands via its external and internal interfaces."
   - **Principle 8.2**: "Systems are resilient and fail-safe if safety-critical functions are compromised or cease to work."

Conclusion

Increased vehicle connectivity means higher risks for OEMs and motorists. Over the past few years, high-profile hacks have led to a flurry of standards setting and regulatory activity outlining how automakers should implement multiple levels of vehicle cyber security solutions to address a wide range of potential threats. To create a clear path towards addressing each of the principles, guidelines and proposed mandates, automakers should adopt comprehensive strategies that align with the NIST cyber security framework.

Argus offers automakers a holistic suite of solutions designed to secure vehicles throughout their lifetime by providing a system for identifying, protecting, detecting, responding and recovering from cyber-attacks. Argus has positioned itself to be a one-stop shop enabling automakers to reduce the risk of security gaps and comply with an increasing roster of cybersecurity standards, guidelines and emerging regulations.