SentinelOne®

CHARLESTON
SCHOOL OF LAW

Charleston CyberLaw Forum

January 18, 2024

SentinelOne

CHARLESTON
SCHOOL OF LAW

Autos and Cyber?

The Auto Transportation Attack Surface and Legal Liability

ALSTON & BIRD

LS Lowenstein Sandler

Secureworks

CHARLESTON
SCHOOL OF LAW

SentinelOne®

Presentation Agenda

1. NHTSA
2. Strict Liability
3. Lawsuits
4. Cybersecurity
5. Future Challenges

The CLE materials are sponsored by SentinelOne and Charleston Law School. All CLE materials are prepared by law firms and attorneys as noted in the materials, and do not offer any specific legal advice or guidance.

Presenters

Todd Benoff

Alston Bird

ALSTON & BIRD

Amy Mushahwar

Lowenstein Sandler
Moderator

LS Lowenstein Sandler

Michael Bryant

Secureworks

Secureworks

NHTSA Is Being Very Cautious

- Understands the need for a single set of regulations
- Respectful of states' traditional areas of authority

Areas NHTSA Has Left to the States

- Licensing and Registration
- Traffic Laws and Enforcement
- Insurance
- Liability

Strict Liability Is Not a Good Fit for AVs

- **Best in class products can be found “defective”**
  - **Risk / Benefit Test**
  - **Consumer Expectations Test**
- **We have never held drivers strictly liable**

Cyberattacks and Strict Liability

- **Suppose your components are part of an attack surface**
  - **Ransomware or DDOS**
  - **Accident**
    - Takes control of the vehicle
    - Spoofs the vision system

How Is Any of This Fair?

- Strict liability has been applied to other criminal acts that are “foreseeable”
- Rock thrown from an overpass penetrates a truck’s windshield (*Collins v. Navistar, Inc.,* (2013) 214 Cal.App.4th 1486, 1504)
- Hacking is “foreseeable”

Strict Liability Is Not Supposed To Be Absolute Liability

- Trucks don’t have to be built like tanks so nothing can get through the windshield
- We’re already seeing people say that connected cars should be cyber-tanks

“Fear of Hacking” Lawsuits

- Fear of hacking class action against Ford, GM and Toyota
- No source authentication or encryption built into CAN packets
- *Cahen v. Toyota Motor Corporation, et al.* (N.D. Cal. Case No. 15-cv-01104-WHO)
- Standing was the only bar

Lawsuits Based on Researcher Exploits

- Miller and Valasek's famous Jeep exploit
- Recall followed by a class action lawsuit
- Alleged defects: hackability, remote control, and inability to patch
- *(Flynn et al. v. FCA US LLC)*

There Is a Lot of General Guidance for Cybersecurity

- **NHTSA (and others) set broad goals**
  - **“Best Practices”**
  - **“Industry Standards”**
- **There is no clear and specific design target**

Complete Domain Separation Is Not Possible

OBD II Port / Dongles

V2X in CAVs

OTA Updates

How Do We Solve These Problems?

- **Work together to change the laws**
- **Protect the people who build safety systems from strict liability**
  - **Negligence**
  - **Special “Connected Car Courts”**

We Have Used These Solutions Before to Save Lives

- **Childhood Vaccines**
  - Low profit margins and lawsuits drove manufacturers out of business
  - Congress created special rules, courts, and compensation programs

What Could Happen Next?

- **New Tactics From the Plaintiffs' Bar**
  - Hiring their own "researchers" to solve the standing problem
  - Arguing that all Level 3 vehicles are "defective"
  - Targeting Auto ISAC and other collaborative groups for discovery
- **Regulators Expand Their Reach**
  - Tesla's FSD as a gateway to regulating ADAS

Clash of the Security Legal Standards?

Vehicle Development Networks

Strict Scrutiny?

Corporate Network

Negligence?

?

What about connected dependencies??

Without regard to the standard, what do I need to do?

What are the actual standards?

Why do I need compliance infrastructure for strict scrutiny analysis? (avoidance of punitive damages)

Security Concerns Are Not Theoretical

Studies, Security Conferences, News and OEM reports are helping define the art of what security issues are foreseeable in AV hardware tech and the Artificial Intelligence that powers the act of driving. Take for example, this helpful study from the EU Agency for Cybersecurity.

CISA's Autonomous Ground Vehicle Security Guide

- **Examines threat vectors within:**
  - **A Vehicle:**
    - Operations and Communications Systems
    - Sensors
  - **Vehicle fleets**
  - **Dependent corporate enterprises**
  - **Supply chain risk**
- **Provides practical guidance to operationalize security that we will delve into next**

AUTONOMOUS GROUND VEHICLE SECURITY GUIDE: Transportation Systems Sector

DEFEND TODAY, SECURE TOMORROW

AUTONOMOUS GROUND VEHICLES IN THE TRANSPORTATION SYSTEMS SECTOR

Autonomous vehicle (AV) technology will revolutionize how people and goods move within communities and across the country. Although fully autonomous vehicles are not common in the transportation landscape,[1] many companies and communities are carrying out pilots for supervised semi-autonomous trucks, shuttles, and delivery services. The U.S. Department of Transportation (USDOT) estimates that more than 80 companies are currently testing AVs across 40 U.S. states and Washington, D.C., and more than half of states have introduced legislation to allow testing on public roads.[2]

AVs represent a leading-edge technology in the evolution of 'Smart Cities,' where infrastructure relies on Internet of Things (IoT) devices to operate effectively. This includes AVs as a viable means for trucking, last-mile delivery, and mass transit—often referred to as mobility-as-a-service—which can benefit organizations and communities through improved mobility, access, and speed; decreased environmental impacts; enhanced safety; improved public transit options; reduced operating costs; and a shift from fixed-route, fixed-timetable services to dynamic, on-demand services.

But in addition to their benefits, these cyber-physical systems (CPS) can also increase vulnerability to physical and cyber attacks at the enterprise and asset level. The Cybersecurity and Infrastructure Security Agency (CISA) developed this product to help Chief Security Officers (CSOs) and Chief Information Security Officers (CISOs) understand the risks associated with AVs and implement strategies that can greatly reduce risk to people and property.

AV Technology in Action

In 2020, the NURO R2 became one of the first autonomous driving systems deployed on public roadways, making it a benchmark for AVs in the transportation landscape.

Source: nhtsa.gov/press-releases/nhtsa-grants-nuro-exemption-petition-low-speed-driverless-vehicle

Components and Systems Context

This graphic illustrates the components and systems that connect AVs to the environments in which they operate.

Navigational uplink

Sync with command and operation center

Sync with smart systems like traffic coordination

Communicate and sync with other AVs

Sensors detect pedestrians, non-autonomous vehicles, traffic signals and signs, and road obstructions

Operation and Communication Systems

Vehicle-to-everything (V2X) Technologies, such as 5G, enable communication to and from an AV system.

Parallel computing enables advanced information processing from vehicle sensors and operating systems.

Dedicated Short Range Communications (DSRC) communicate and sync capabilities with other AVs.

Global Navigation Satellite Systems / Inertial Navigational Systems (GNSS/INS) ensure accurate position, velocity, acceleration, and heading data for autonomous operation.

Sensor Systems

Light Detection and Ranging (LiDAR) uses light pulses to estimate distance and create high-resolution 3D images of the environment and road.

High-frequency acoustic sensors use audio waves to measure distance to an object.

Radio Detection and Ranging (RADAR) relies on radio waves to enable braking assistance applications and sensors that monitor blind spots for distance control.

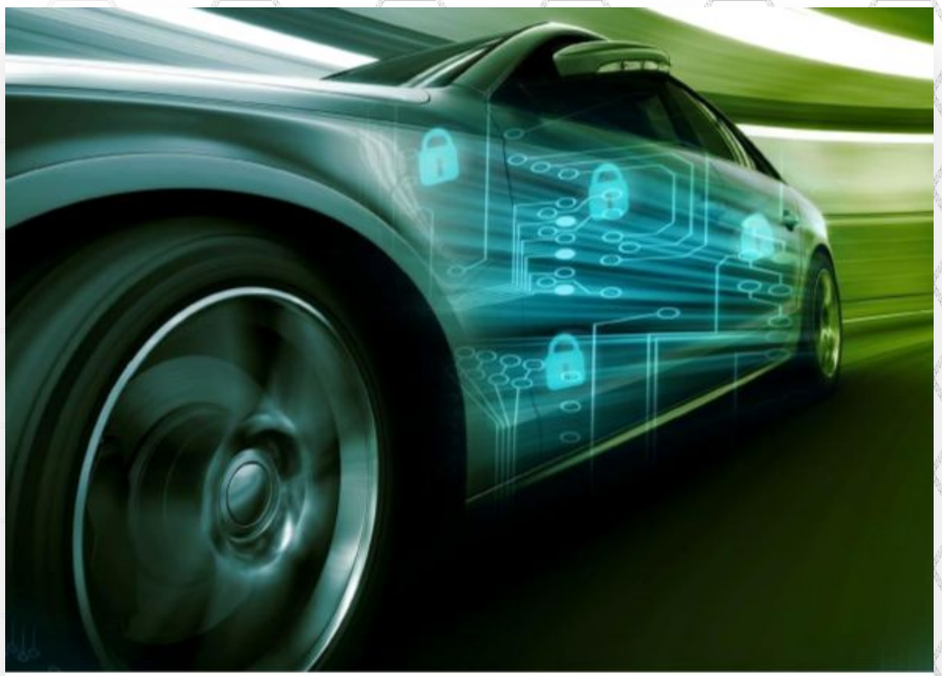
Monocular cameras allow an AV to gather 3D images of its surroundings.

Stereo cameras capture images from two viewpoints to triangulate depth information.

Traffic-sign Recognition (TSR) uses forward-facing cameras to recognize and interpret traffic signs on roadways.

AUTO-ISAC Cybersecurity Best Practices

- **Provide a basic NIST application to the automotive development process for pre- and post-production vehicles. Focuses on the following best practices:**
  - Incident Response
  - Vendor Collaboration
  - Governance
  - Risk Assessment and Management
  - Awareness and Training
  - Threat Detection, Monitoring and Analysis
  - Secure Development Lifecycle



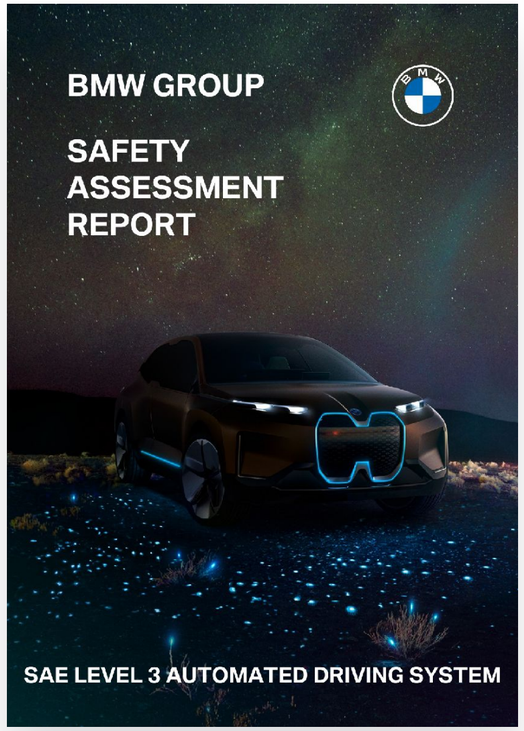
Cyberia Key Component in the New Automated Driving Systems Standards

- **NHTSA continues to recommend:**
  - **Systematic and ongoing safety risk assessment for each ADS (for vehicle design and broader connected ecosystem, if necessary)**
  - **Follow established cyber practices of:**
    - NIST
    - NHTSA
    - SAE International
    - Alliance of Automanufacturers
    - Association of Global Automakers
    - Auto-ISAC (we discussed)

Cyber Statements in Current NHTSA Voluntary Reports

OEMs

- **BMW –** Defense in depth strategy, excellent substance (included below)
- **GM –** Recognition of connected services, mobile apps and in-vehicle app security as well as active fleet management

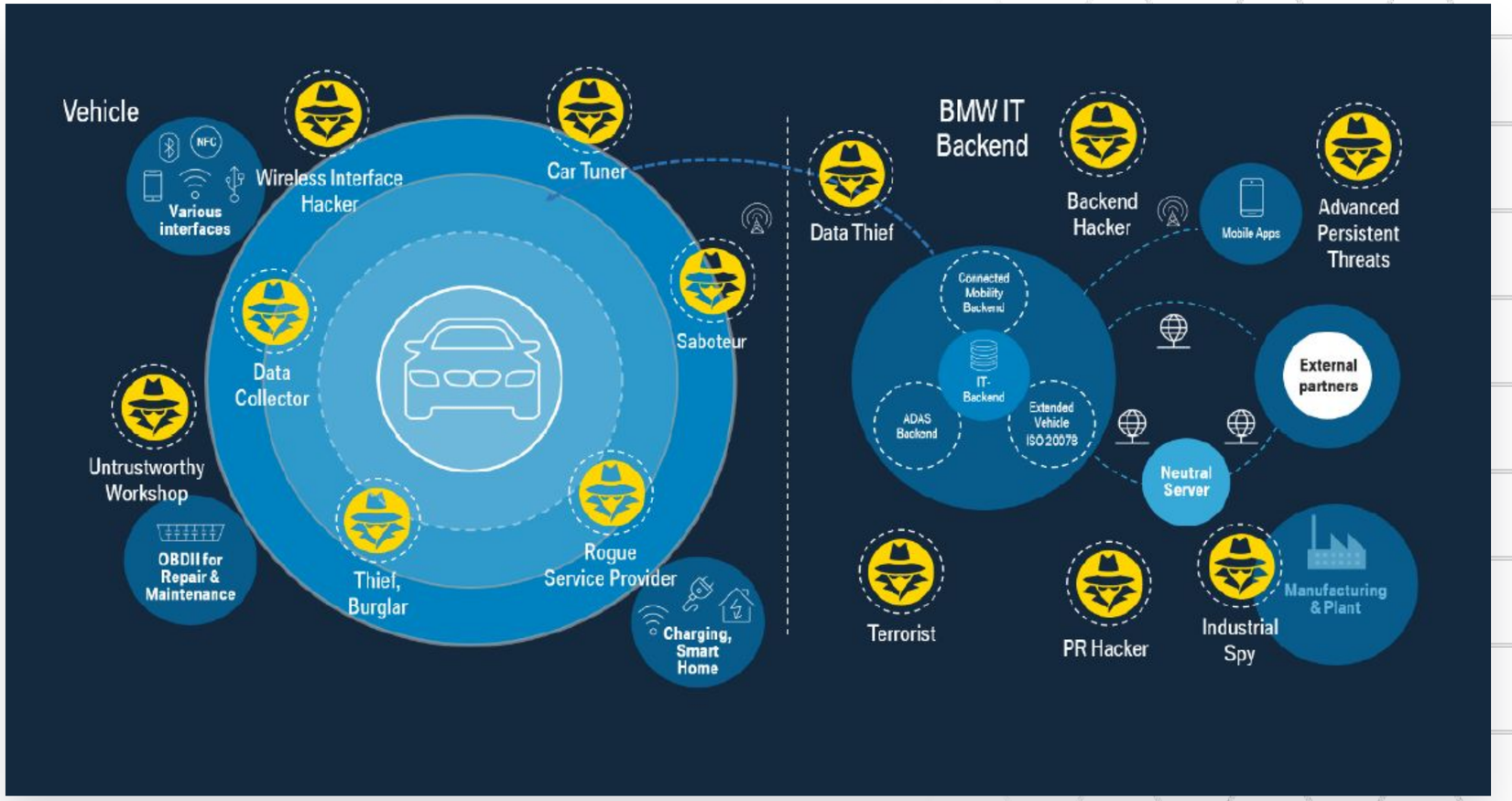


Tech Companies

- **Argo AI and Nuro –** NIST Cyber Framework model
- **EasyMile –** SAE J3061 model
- **Kodiac –** NIST Cyber Framework and NHTSA Cyber Best Practices model
- **Motional –** Focused on SDLC components that we will discuss

BMW's Representation of the Vehicle Threat Ecosystem

Please see page 46 of the provided BMW Voluntary Report

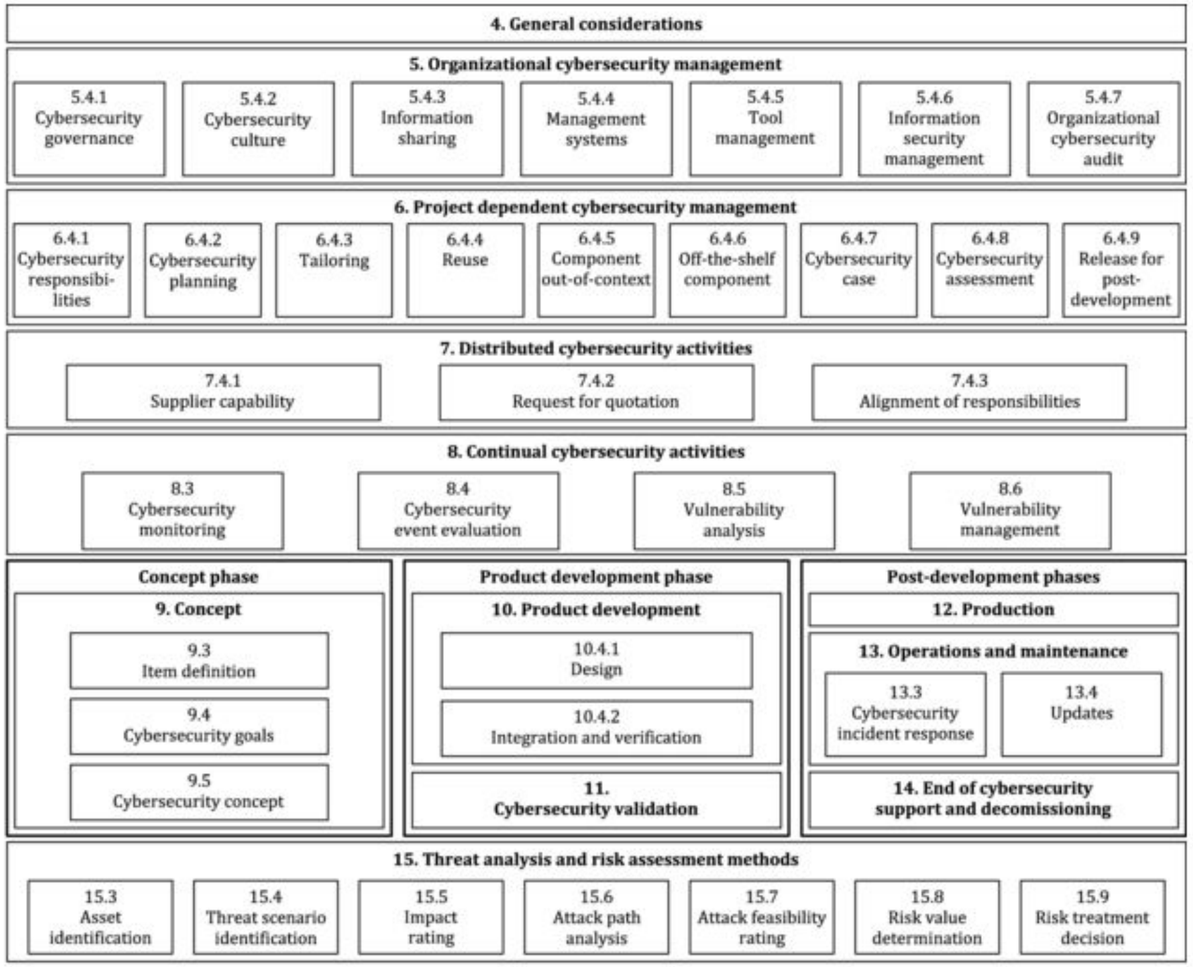


ISO/SAE 21434:2021

Looks Familiar for Security GRC

The newer ISO AV standard has a familiar security governance structure, but there is much room for interpretation. This means that OEMs and technology providers are left with some uncertainty as to how to apply general security concepts to AV operational technology.

Figure 1 — Overview of this document



How Do You Demonstrate Security Maturity?

- **Program Governance**
  - WISP
  - Board minutes and key updates
  - Budget
- **Risk Assessment**
  - Threat intelligence
  - Annual risk assessment
  - SDLC documentation and security consideration
  - Security/Internal Audits
  - POAMs (Plan of Actions & Milestones) / Risk Registers
  - Third-party certifications
- **Training (general security awareness, cyber-physical incidents, merge understanding of corporate security with OT)**
- **Incident Response (plans, documentation and tests)**

Key Risk Areas

Legal Ask for Information On….

- Secure Development Lifecycle
- Network and Systems Architecture
- Access Controls
- Change Management/Project Management
- Disaster Recovery
- Patch and Vulnerability Management
- Vendor Risk Management
- Insider Threat Management

Data Privacy Concerns for Driverless Cars

What information do driverless cars collect?

- **Basic personal information (name, email address, home address, phone number, etc.)**
- **Biometric and behavior analytic data (face scans, fingerprints, voiceprints, iris scans, etc.)**
- **Geolocation (enhanced data)**
- **AI-based data**

Why is this data valuable?

- **Advertisers**
- **Insurance companies**
- **Mobile app developers**
- **OEMs and infrastructure operators**
- **Roadside assistance providers**
- **Law enforcement**

The Driverless Car Industry is Becoming a Highly-Regulated Industry:

- **Comprehensive Privacy Legislation –** EU's GDPR, China's PIPL, Brazil, South Korea, and California's CCPA/CPRA
- **U.S. Autonomous Driver-specific Privacy Laws –** 40 states and Washington, D.C. have enacted legislation or issued executive orders related to autonomous vehicles
- **Federal Trade Commission –** Enforces privacy and cybersecurity violations through Section 5 of the FTC Act

SentinelOne

CHARLESTON SCHOOL OF LAW

Amy Mushahwer

Chair, Data Privacy & Security, Lowenstein Sandler LLP

Lowenstein Sandler

Amy advises clients on proactive data security practices, data breach incident response, and regulatory compliance. She handles security incidents and has interacted with federal and state agencies and forensic service providers, overseen investigations, and designed post-incident response notification and remediation plans.

In addition to her incident response work, Amy provides compliance support on applicable security laws, PCI-DSS, and security audit standards such as NIST. She also facilitates in-depth security incident simulations. Amy is a former technology consultant and chief information security officer (CISO), and previously owned and operated a technology consulting company.

Todd B. Benoff

Partner, Privacy, Cyber & Data Strategy, Alston & Bird

ALSTON & BIRD

Todd Benoff focuses his trial practice on high-exposure cases in the areas of products liability, toxic torts/mass torts, and business litigation, including complex False Claims Act matters and consumer class actions. He also focuses on cybersecurity issues presented by connected and autonomous vehicles.

In his products liability and toxic tort work, Todd has defended manufacturers of cars, trucks and trailers, as well as electrical distribution products, specialty chemicals and water distribution systems and components. Todd handles a wide array of business litigation matters, including consumer class actions, unfair business practice claims, contract disputes, shareholder derivative actions, and disputes involving real estate purchases and investments. Todd also practices at the appellate level.

Todd has been recognized by The Best Lawyers in America© (2023 and 2024) and was selected to the “Rising Stars” list by Southern California Super Lawyers (2007–2012). He received both his B.A. and J.D. from the University of Virginia in 1994 and 1997, respectively.

Michael Bryant

Sr. Manager, Secureworks

Secureworks

Michael Bryant is a Senior Consultant and penetration tester with SecureWorks Adversary Group. He has over twenty-two years of experience in the information security field, including both offensive, defensive and compliance roles. He holds both an Offensive Security Certified Professional (OSCP) and CISSP certification and graduated from Clemson University with a degree in Electrical Engineering.

SentinelOne®

CHARLESTON
SCHOOL OF LAW

Thank You