NHTSA’S AUTOMOTIVE CYBERSECURITY RESEARCH

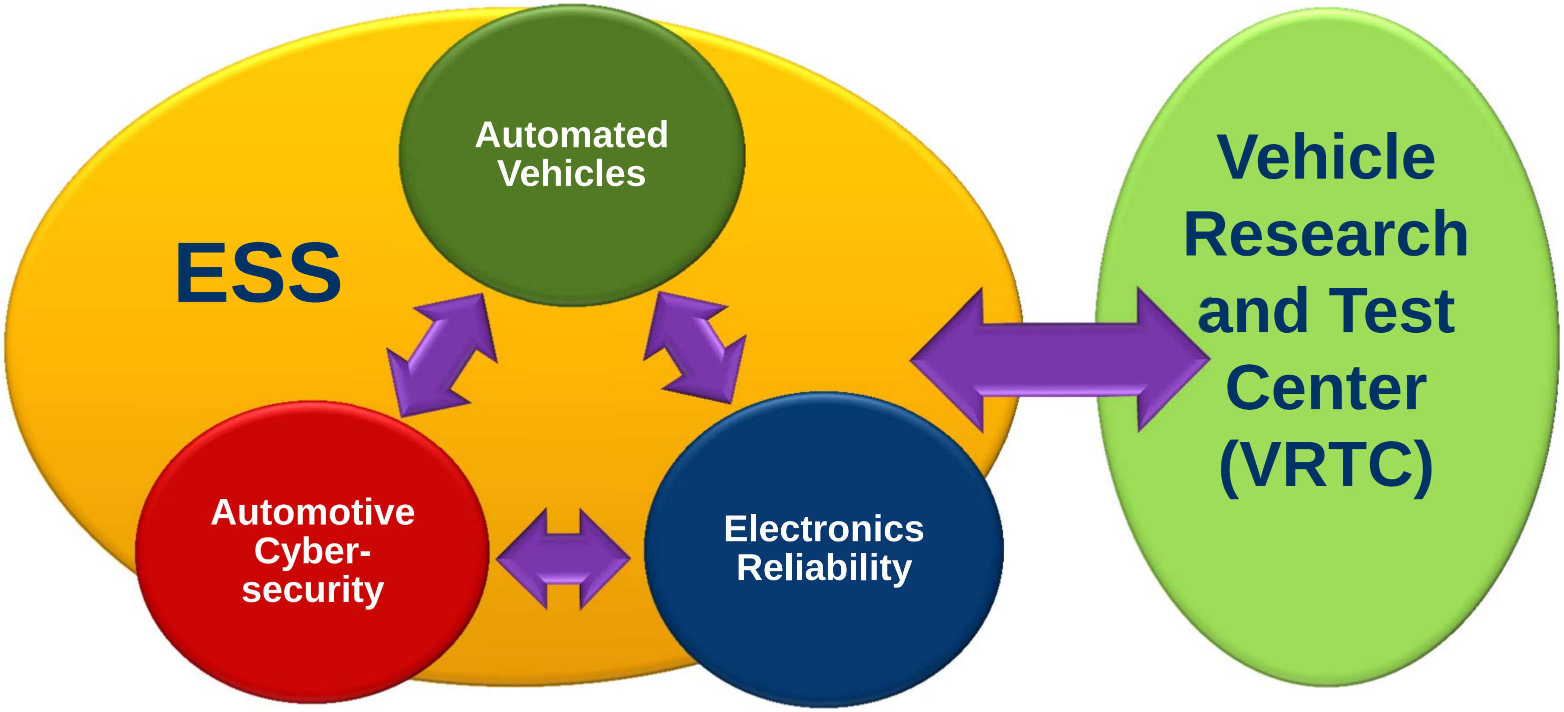
Arthur Carter, Frank Barickman, NHTSA

INTERNATIONAL

www.nhtsa.gov

Electronic Systems Safety Research Division

Electronic Systems Safety (ESS) Research Division conducts research to ensure the safety, security and reliability of the interconnected, complex electronic systems. ESS is also responsible for leading the agency's research in the continuum of automated driving.


Automated Vehicles
ESS
Automotive Cyber-security
Electronics Reliability
Vehicle Research and Test Center (VRTC)

Threat Vectors into Automotive Systems

- **Physical and Remote access into the vehicle:**
  - Physical interfaces
  - Short Range wireless interfaces
  - Long range wireless interfaces

- **With prolonged physical access, researchers demonstrated in specific cases access via:**
  - Ports: OBD-II, CD/DVD Players, USB, etc.
  - Certain Vehicle data bus types (e.g. Controller Area Network – CAN) that interconnect vehicle electronic and controls systems
  - Wireless: Key FOBs, Wi-Fi, Bluetooth, etc.

Automotive Cyber Threat Generalization Difficult

- **Original Equipment Manufacturers (OEMs) design their platforms differently**
  - There are many architectural variations
  - Many are proprietary
  - The platform designs are constantly evolving

- **OEMs more proactive in design-for-security**
  - Private discussions with OEMs and Tier 1s

- **Functional Safety is closely coupled with Automotive Cybersecurity**

NHTSA’s Integrated Research Approach

- **Build a Cybersecurity Knowledge Base**
  - Identify key stakeholders, lessons learned from other industry sectors, and gap areas in need of further research
  - Facilitate coordination and information exchange
- **Support the development of industry standards, guidelines, and best practices**
  - Outreach and influence industry through SAE International and other industry groups, at industry conferences, etc.
- **Research minimum technical requirements**
  - Systematic vehicle security assessment approach
  - Study vehicle architectures and threat vectors and risks
  - Test and evaluate automotive cybersecurity environment
  - Complete research supportive of future technical requirements
- **Cybersecurity policies, regulations, principles**
  - Research alternatives, certification and enforcement challenges

Testing Capabilities

Building capabilities to support in-house NHTSA applied cybersecurity research.

- Projects’ objectives are driving laboratory capabilities

VRTC Cybersecurity

Capabilities

- Communication bus monitoring
- RF monitoring
- GPS Spoofing
- GPS Simulation
- Firmware Analysis

Equipment

- Vector CANalyzer
- Roller Dynamometer
- USRP Software Defined Radio
- GPS Satellite Simulator
- Spectrum Analyzer
- IDA Pro

Future Capabilities

- Femtocell/cellular base transceiver station
- RF Disruption
  - LTE
  - DSRC
  - GPS
  - Radar

Task for NHTSA : Assessment of the Need for New Safety Standards (Electronics)

- **The Moving Ahead for Progress in the 21st Century Act (MAP-21) Division C, Title I, Subtitle D, Section 31402 requires that the agency examine the need for safety standards with regard to electronic systems in passenger motor vehicles. Act directed the agency to**
  - consider the electronic components; the interaction of electronic components; the security needs for those electronic systems to prevent unauthorized access, and the effect of surrounding environments on the electronic systems, allow public comment.
- **MAP-21 also requires that the agency submit a report to Congress on its findings pursuant to the examination referenced above. Current Status: The agency published a Federal Register Notice on Electronic system safety and security on October 7, 2014. Public comments were due December 8, 2014.**
  - Presents our research program and progress on examining the need for safety standards with regard to electronic systems in passenger motor vehicles. Public comments are being assessed.

Federal Register Notice (Cybersecurity side)

- **Process-oriented approaches to addressing cybersecurity concerns**
  - Design and quality control processes that focus on cybersecurity issues throughout the lifecycle of a product.
  - Dealing with cybersecurity issues through establishing robust information sharing forums such as an Information Sharing and Analysis Center (ISAC).

- **Generally a cycle of cybersecurity activities are implied; Layered approach**
  - Prevention Methods (gateways, isolation, authentication)
  - Detection Methods (e.g. Anomaly based intrusion detection)
  - Reaction Methods (containment; e.g. shut down sys/communications)
  - Treatment Methods (distribute knowledge to others)

- **Follow-up with a report to congress next year**

NHTSA Cybersecurity Reports

- **NHTSA Released four Automotive Cybersecurity Reports in October 2014**
  - Assessment of the Information Sharing and Analysis Center Model;
  - A Summary of Cybersecurity Best Practices;
  - Characterization of Potential Security Threats in Modern Automobiles: A Composite Modeling Approach; and
  - National Institute of Standards and Technology Cybersecurity Risk Management Framework Applied to Modern Vehicles

Report: “Assessment of the Information Sharing and Analysis Center(ISAC) Model”

- **An ISAC is a trusted, sector-specific entity that can provide a 24-hour per day and 7-day per week secure operating capability that establishes the coordination, information sharing, and intelligence requirements for dealing with cybersecurity incidents, threats, and vulnerabilities.**
  - An ISAC can serve as an industry resource to gather key information about cybersecurity events and issues and identify, communicate, and analyze potential impacts of such concerns to the industry.
  - How ISACs are implemented in other sectors;
  - How existing ISACs can be leveraged to expeditiously form of a new sector ISAC.
  - Report sent to Global/Alliance to aid with their Auto-ISAC activities

Report: “A Summary of Cybersecurity Best Practices”

- **Documents results from the analysis and review of best practices and observations across a variety of industry segments in the field of cybersecurity involving electronic control systems;**
  - Provides relevant benchmarks for the Agency and the industry; This information helps
    - Increase the collective knowledge base in automotive cybersecurity;
    - Identify potential knowledge gaps;
    - Describe the risk and threat environments;
    - Support follow-on tasks used to establish security guidelines.

Report: "Characterization of Potential Security Threats in Modern Automobiles"

- **Describes a composite modeling approach for potential cybersecurity threats in modern vehicles. Threat models, threat descriptions, and examples of various types of conceivable threats to automotive systems are included, along with a matrix containing a condensed version of the various potential attacks.**
  - Threat models, descriptions, and examples of various types of threats to automotive systems are included, along with a matrix containing a condensed version of the various sample attack possibilities.
  - A Composite Threat Model is presented
  - Contains common elements from various methods examined.
  - Use cases are studied

Report: “NIST Risk Management Framework Applied to Modern Vehicles”

- **Reviews the NIST guidelines and foundational publications from an automotive cybersecurity risk management stand-point. The NIST approach is often used as a baseline to develop a more targeted risk management approach for the specific use cases and issues in specific industries and sectors.**
  - The Risk Management Framework provides a 6-step structured process that integrates information security and risk management activities into the system development life cycle. Tailored to modern vehicles:
    - Assess Threats via Use Cases
    - Categorize Vehicle Systems
  - Confidentiality, Integrity, and Availability, with requirement levels of Low, Moderate, High, and Not applicable are used for each
    - Select Security Controls
    - Implement Security Controls
    - Assess Security Controls
    - Monitor Security Controls (Repeat)

Summary

- Encouraging the development of an <u>*Automotive ISAC*</u>
- Continuing to <u>coordinate with key stakeholders</u>
  - Standards organizations, private and public sector information exchanges
    - FR notice comments being processed
    - Holding discussions with OEMs, Tier 1s, Tier 2s, Safety Critical System Developers in other sectors etc.
    - Other Federal and State Agencies:

      - NHTSA holding a Cyber Roundtable on Feb 13, 2015.

Summary

- <u>**Technical Research**</u>
  - Monitoring SAE Automotive Cybersecurity Guidelines development effort
  - Planning to expand cybersecurity research to include higher levels of automation
  - Initiating research into anomaly based intrusion detection systems' capabilities and effectiveness
  - Applied Research into cybersecurity related testing

- **Main goal: Development of security requirements or guidance for safety assurance of critical automotive systems based on foundational research results**

NHTSA Resources

- **Federal Register Notice on Electronic Systems Safety and Security**
  - http://www.regulations.gov/#!docketDetail;D=NHTSA-2014-0108
- **NHTSA's crash avoidance research technical publications are posted at:**
  - http://www.nhtsa.gov/Research/Crash+Avoidance/Office+of+Crash+Avoidance+Research+Technical+Publications
- **ESS research reports, related public documents will be placed in the following non-rulemaking dockets:**
  - **NHTSA-2014-0070**: Vehicle Automation Topics and Publications
  - **NHTSA-2014-0071**: Automotive Cybersecurity Topics and Publications
  - **NHTSA-2014-0092**: Automotive Functional Safety and Reliability Topics and Publications
- Dockets can be accessed at http://www.regulations.gov/

Contact Information

- **Art Carter**
  - Program Lead, Automotive Cybersecurity, ESS, NHTSA
  - Phone: 202-366-5669
  - E-mail: arthur.carter@dot.gov

- **Frank Barickman**
  - Electronics Team Lead, Vehicle Research and Test Center, NHTSA
  - Phone: 937-666-3315
  - E-mail: frank.barickman@dot.gov