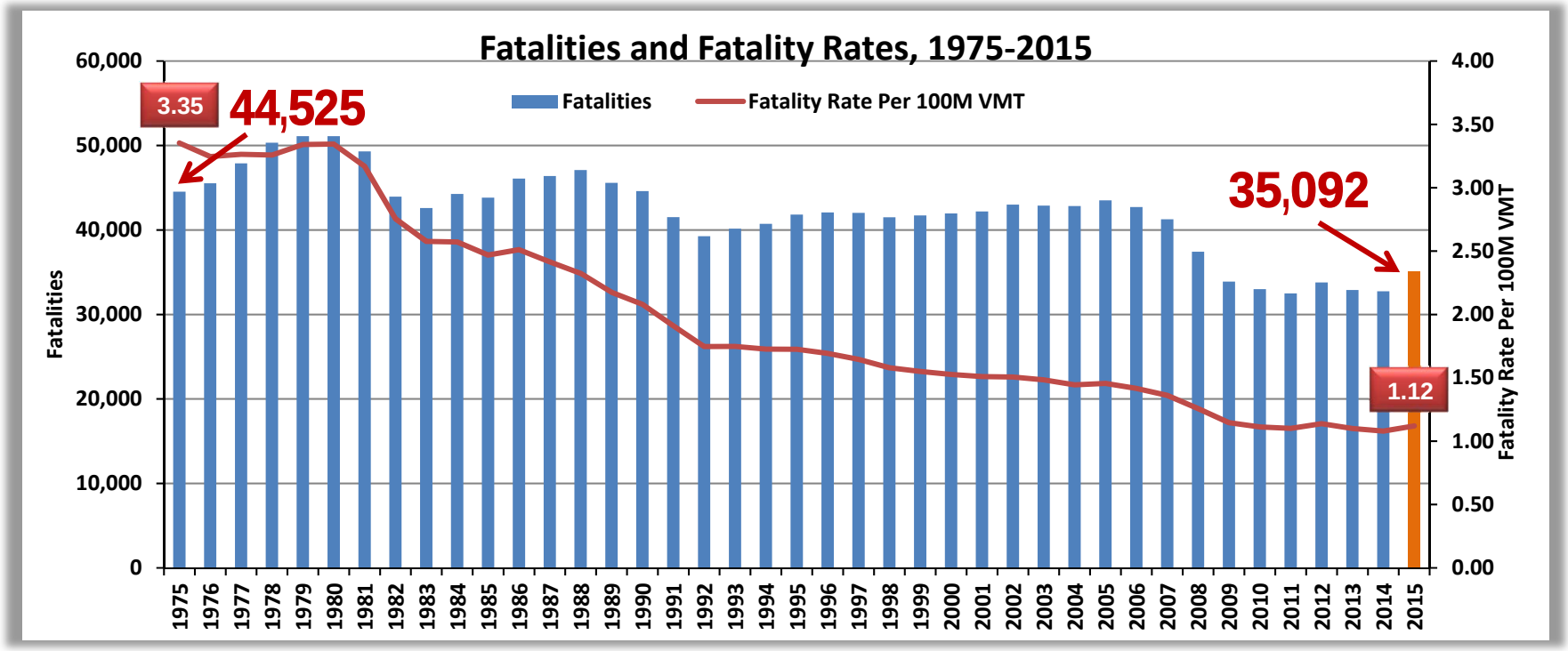
CYBERSECURITY BEST PRACTICES FOR MODERN VEHICLES

Cem Hatipoglu, Ph.D.
Director, Office of Vehicle Crash Avoidance
and Electronic Controls Research

NHTSA
NATIONAL HIGHWAY TRAFFIC SAFETY ADMINISTRATION

SAE
INTERNATIONAL

Fatalities and Fatality Rate, by Year

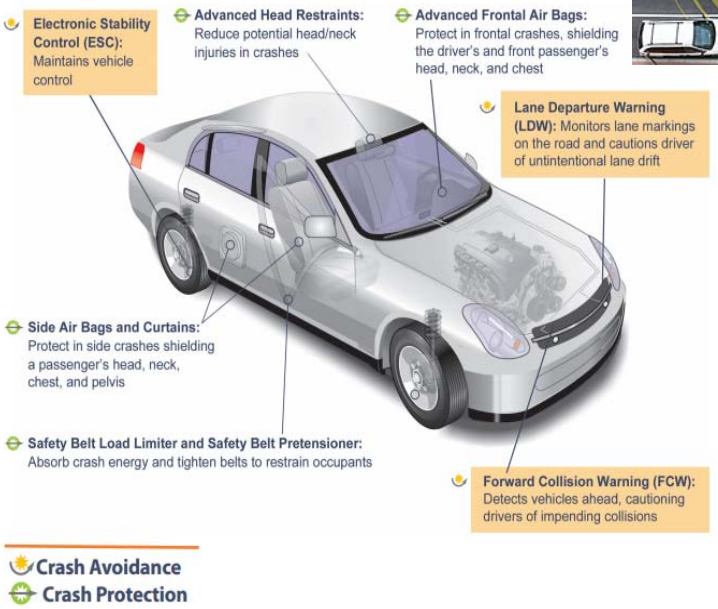


Motor vehicle crashes cost nearly $836 billion

Continued Technological Innovations…

35,092 people lost their lives due to motor vehicle accidents in 2015

- **Modern crash avoidance, vehicle-to-vehicle (V2V) communications, and automated vehicle technologies hold the promise to address most crash challenges.**



The Need for Cybersecurity Research

However, these safety features introduce **new cybersecurity challenges and vulnerabilities** as demonstrated by our research and that of others.

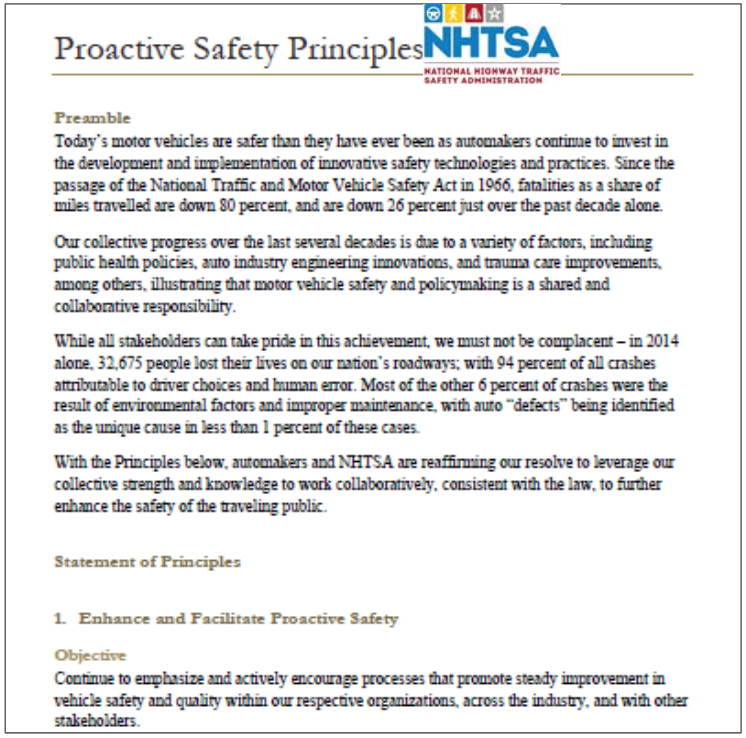
Failure to tackle the cybersecurity challenge would threaten the **technology-driven safety transformation** we all want to achieve.

Proactive Safety Principles

NHTSA finalized a historic agreement with 18 automakers in January 2016, on proactive safety principles. The signatories agreed to work together to develop a collaborative, data–driven, science–based process, consistent with the law, to advance safety objectives.

Vehicle Cybersecurity Specific Objective: *Explore and employ ways to work collaboratively in order to mitigate those cyber threats that could present unreasonable safety risks.*

- **Best practices that reflect lessons learned within and outside of the auto industry to foster enhanced cyber resiliency and effective remediation. Executive summary recently released.**
- **Support and evolve the auto industry's information sharing and analysis center (Auto–ISAC), enhance it over time and expand its membership**



Proactive Safety Principles NHTSA
NATIONAL HIGHWAY TRAFFIC SAFETY ADMINISTRATION

Preamble

Today's motor vehicles are safer than they have ever been as automakers continue to invest in the development and implementation of innovative safety technologies and practices. Since the passage of the National Traffic and Motor Vehicle Safety Act in 1966, fatalities as a share of miles travelled are down 80 percent, and are down 26 percent just over the past decade alone.

Our collective progress over the last several decades is due to a variety of factors, including public health policies, auto industry engineering innovations, and trauma care improvements, among others, illustrating that motor vehicle safety and policymaking is a shared and collaborative responsibility.

While all stakeholders can take pride in this achievement, we must not be complacent – in 2014 alone, 32,675 people lost their lives on our nation's roadways; with 94 percent of all crashes attributable to driver choices and human error. Most of the other 6 percent of crashes were the result of environmental factors and improper maintenance, with auto "defects" being identified as the unique cause in less than 1 percent of these cases.

With the Principles below, automakers and NHTSA are reaffirming our resolve to leverage our collective strength and knowledge to work collaboratively, consistent with the law, to further enhance the safety of the traveling public.

Statement of Principles

1. Enhance and Facilitate Proactive Safety

Objective

Continue to emphasize and actively encourage processes that promote steady improvement in vehicle safety and quality within our respective organizations, across the industry, and with other stakeholders.

January 2016 Event

- **Four Panels**
  - 35 Panelists with different affiliations
    - OEMs, Suppliers, Federal Agencies, Security Researchers, Associations, Advocates, Technology Companies…
- **Audience**
  - Over 300 in attendance
    - Over 200 unique orgs
    - 25 Federal Groups
    - 17 OEMs
    - 13 Associations

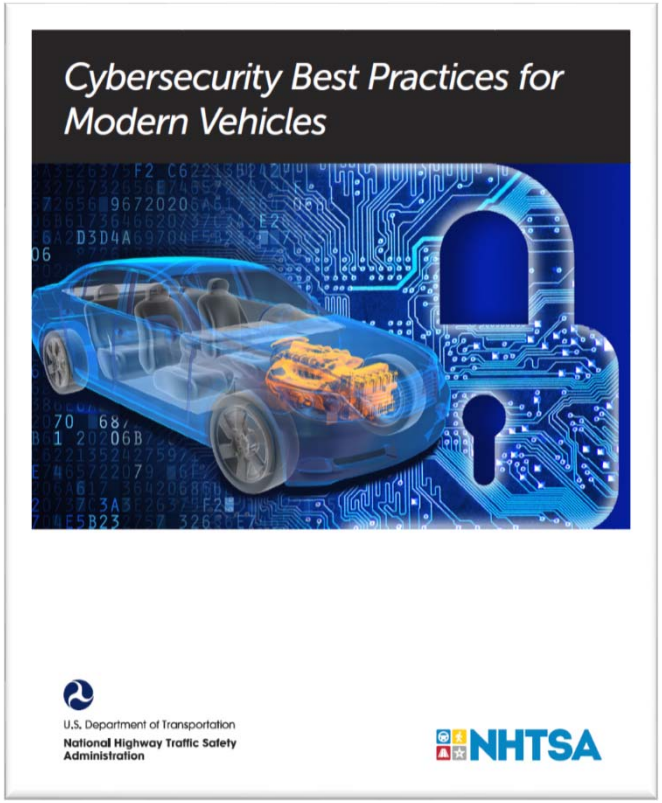
Cybersecurity Best Practices for Modern Vehicles

Released on October 24, 2016

http://www.nhtsa.gov/staticfiles/nvs/pdf/812333_cybersecurityForModernVehicles.pdf

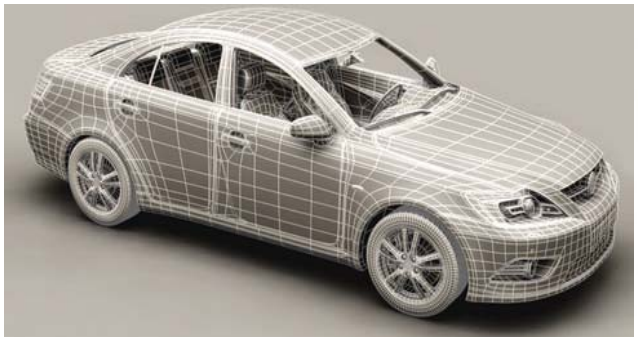
Docket: NHTSA-2016-0104

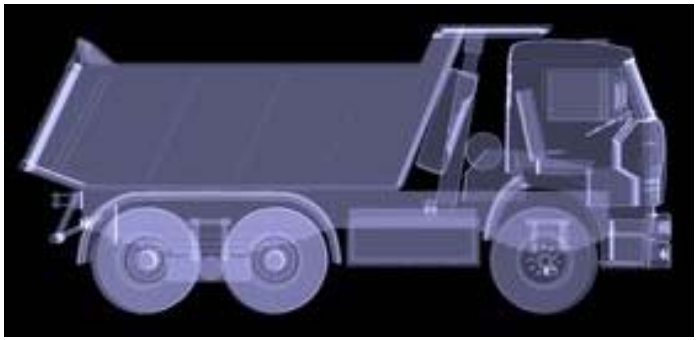
Comment Period Closed on 11/28/2016



Scope- Cybersecurity Best Practices Guidance

- **…all individuals and organizations manufacturing and designing vehicle systems and software.**
- **…all classes of motor vehicles, including passenger cars, trucks and buses**





Document Framework

- **General cybersecurity guidance**
- **Auto-industry specific guidance**
  - Processes
  - Fundamental Protections for Consideration
- **Other guidance**
  - Education, Aftermarket Devices, Serviceability

General Guidance

- **Adopt a risk-based approach**
- **Follow NIST's cybersecurity framework**
  - Identify, Protect, Detect, Respond, Recover
  - Comprehensive and systematic approach to develop layered protections
- **Review and consider IT security suite of standards**
  - ISO 27000 series, CIS CSC

Industry Specific Guidance

- **Vehicle development process with inherent and explicit cybersecurity considerations**
- **Top-down leadership priority on product cybersecurity**
- **Cybersecurity information sharing**
- **Vulnerability reporting policy**
- **Incident response process**
- **Self-auditing**

Fundamental Vehicle Cybersecurity Protections

- Limit **Developer/Debugging Access** in Production Devices
- Control **Keys**
- Control Vehicle Maintenance **Diagnostic Access**
- Control **Access to Firmware**
- Limit Ability to **Modify Firmware**
- **Control Proliferation** of Network Ports, Protocols and Services
- Use Segmentation and Isolation Techniques in Vehicle Architecture Design
- Control Internal **Vehicle Communications**
- **Log Events**
- Control Communication **to Back-End Servers**
- Control **Wireless Interfaces**

Other topics

- **Education**
  - an **educated workforce** is crucial to improving the cybersecurity posture of motor vehicles
- **Aftermarket Devices**
  - devices are interfaced with cyber-physical systems and they could **impact safety-of-life**
- **Serviceability**
  - do not **unduly restrict access** by authorized alternative third-party repair services

Also…

- **Federal Automated Vehicles (FAV) Policy**
  - Released September 2016
- **www.transportation.gov/av**

- **Cybersecurity is called out as one of 15 safety assessment areas**
- **Docket No. NHTSA-2016-0090 (Document No. 2016-22993)**

CEM HATIPOGLU

CEM.HATIPOGLU@DOT.GOV

WWW.NHTSA.GOV