SAFETY ANALYSIS APPROACHES FOR AUTOMOTIVE ELECTRONIC CONTROL SYSTEMS

Qi Van Eikema Hommes, Ph.D.
Advanced Vehicle Technology Division
John A Volpe National Transportation Systems Center
Office of the Secretary of Transportation
U.S. Department of Transportation

January 22, 2015

SAE INTERNATIONAL

Volpe The National Transportation Systems Center

Advancing transportation innovation for the public good

Presentation Outline

- Overview of the Electronics Reliability Research
- On-going Safety Analysis Projects
- Hazard and Safety Analysis Approaches
- Summary

NHTSA's Electronics Reliability Research*

Engage stakeholders, build a knowledge base

- Industry based, voluntary process standards research
- Integrated diagnostics, prognostics capabilities research
- Effective failure response mechanisms research

Identify, define, and prioritize systems that may need new safety requirements

- Develop failure typology for electronic control systems
- Review and evaluate available data sources and their suitability

Develop functional safety requirements for safety-critical automotive control systems

- Hazard Analyses using Hazard and Operability (HazOp) analysis method and System Theoretic Process Analysis (STPA) method
- Safety requirements

Research gaps in functional safety approaches for application to safety-critical electronic control systems, including highly automated vehicles

- Rechargeable energy storage, accelerator/electronic throttle controls, automated lane centering

** Cem Hatipoglu and Dave Freeman, "Government Perspective: NHTSA's Electronics Reliability & Functional Safety Research," International Conference on Managing Functional Safety, 9/16/2014.*

Safety Analysis of Accelerator Control Systems (ACS) / Electronic Throttle Controls (ETC)

Goal

Support the need for additional safety requirements about the failures and countermeasures of the ACS with electronic faults, such as errant ETC signals.

Objectives

- Conduct hazard analysis of electronic-related ACS/ETC failures
- Identify safety requirements and safety constraints

Focus

- Light vehicles (gross vehicle weight rating under 10,000 pounds)
- Seven propulsion system variants: gasoline Internal Combustion Engine (ICE), diesel ICE, Electric Vehicle (EV), Hybrid Electric Vehicle (HEV) with gasoline IC (series, parallel, series-parallel), and HEV with fuel cells.

Safety Analysis of Automated Lane Centering Controls (ALC)

Goal

Ensure the safe operation and functional safety of ALC control systems at all NHTSA automation levels.

Objectives

- Conduct comprehensive hazard analysis
- Define functional safety concepts and requirements
- Propose initial requirements for improving driver awareness and training

Focus

- Light vehicles (gross vehicle weight rating under 10,000 pounds)
- Steering and/or braking lateral controls
- Shared lateral and longitudinal control systems

Safety Management of Automotive Rechargeable Energy Storage Systems (RESS)

Goal

Conduct research in selected areas of hazard analysis and safety management of automotive RESS to improve the technical understanding of these areas and build the foundation for follow-on research.

Objectives

- Understand hazards and severity levels in context of functional safety of RESS Battery Management Systems
- Understand system diagnostics, data logging, and prognostics
- Identify safety-critical information needs and effective methods to communicate this information to operators, first and second responders, and service technicians
- Address safety-related instructions and training needs

Focus

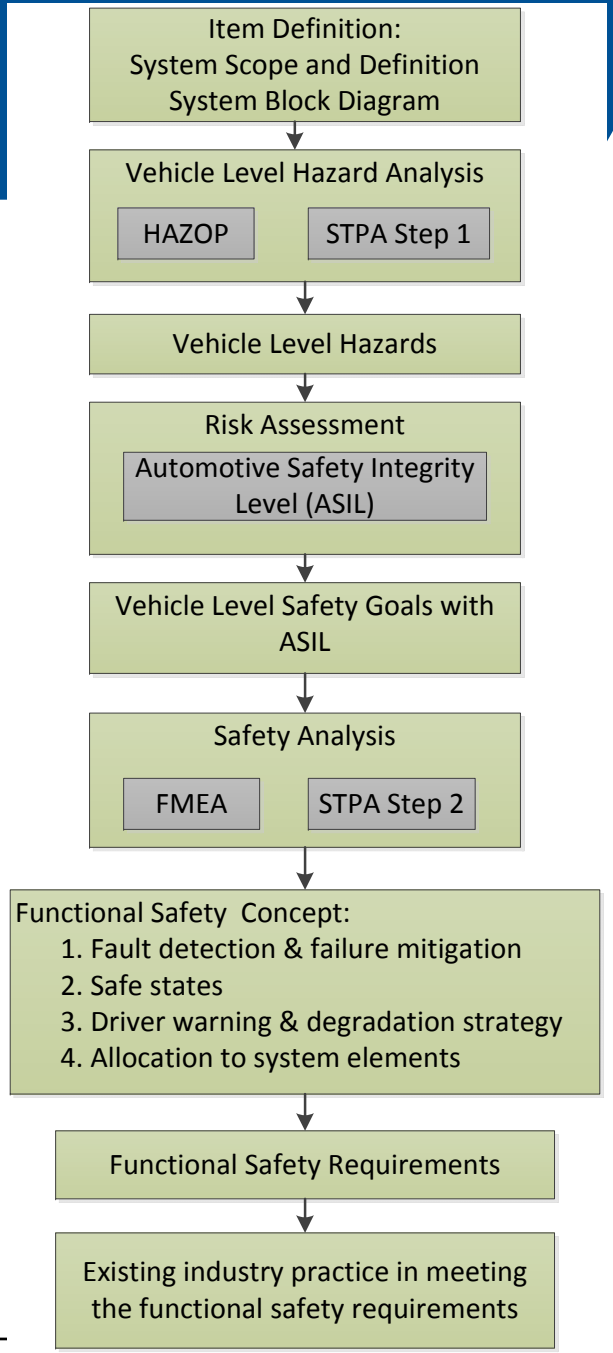
- Light vehicles (gross vehicle weight rating under 10,000 pounds)

Analysis Process and Approaches

- Follow the process in the ISO 26262 Concept Phase.
- Apply multiple approaches for hazard and safety analysis:
  - Hazard and Operability (HAZOP) Analysis
  - Failure Mode and Effects Analysis (FMEA)
  - System Theoretic Process Analysis (STPA)
- Aim to identify a comprehensive list of hazards and causal factors in order to support the development of safety requirements.
- Assess driver-vehicle interaction for vehicle automation levels 2-4.

Note: This presentation will focus on the STPA method, assuming the audience is familiar with HAZOP and FMEA.

**ISO 26262 does not recommend or endorse a particular method for hazard and safety analyses. Other comparable and valid hazard and safety analysis methods may be used at the discretion of the analyst/engineer.*



System Theoretic Process Analysis (STPA)

- A hazard analysis method aimed to identify causes leading to vehicle-level losses
- A top-down systems engineering approach
- Incorporates control system theory
- Considers both component failures and system interactions
- Integrates driver-vehicle interface in the overall modeling
- Assists the identification of software safety requirements
- Provides a well-guided and structured analysis process
- Produces documented and traceable rationales that link component failures and unsafe interactions to vehicle-level hazards and losses
- Generates hazards and causal factors that are inputs to safety requirements and constraints

Analysis Steps

System Description:

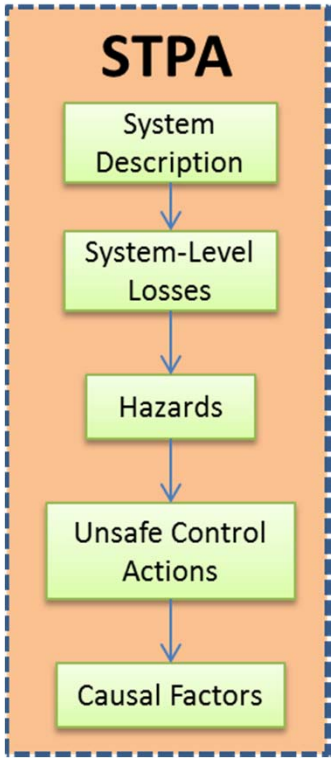
- Functional description
- System scope definition
- control structure of the system (block diagram)

System-Level Loss:

An undesired and unplanned event that results in the loss of human life or injury, property damage, environmental pollution, etc**.**

Hazard:

A system state or set of conditions that, together with a particular set of worst-case environmental conditions, will lead to a system-level loss.



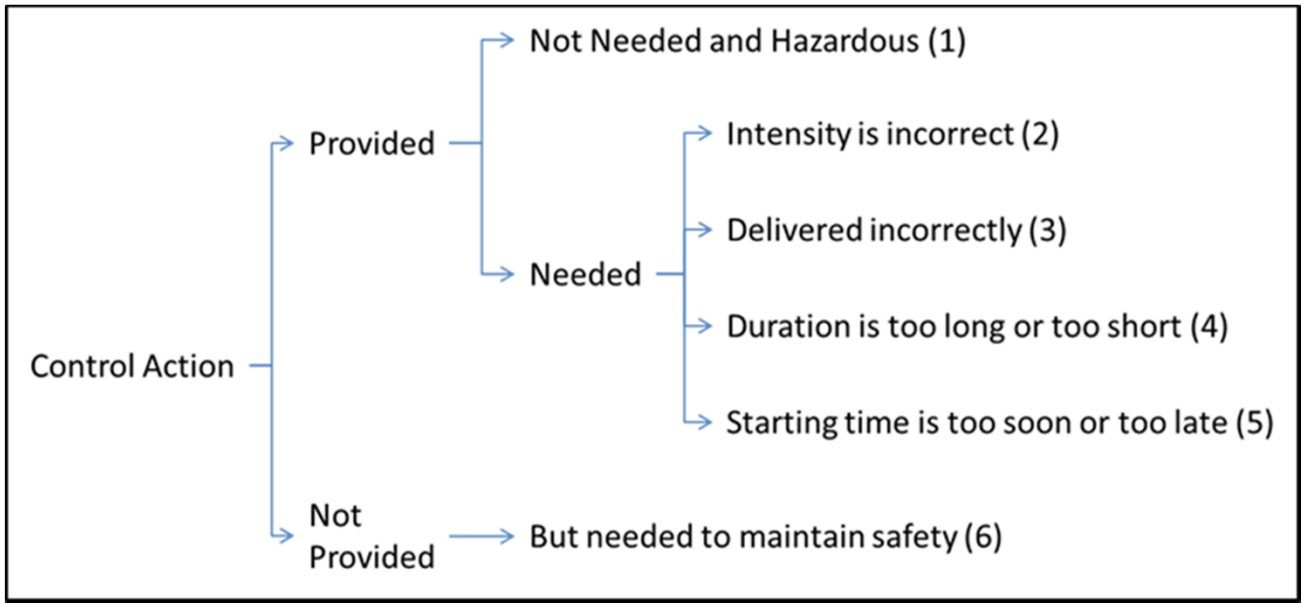
STPA Step 1: Unsafe Control Actions

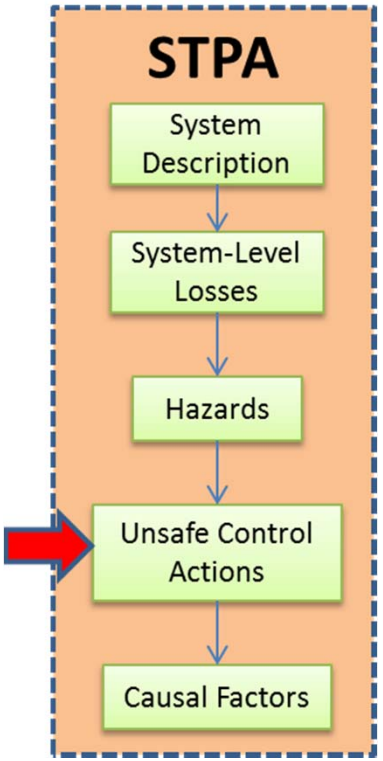
Unsafe Control Actions (UCAs) are commanded by controllers that can potentially cause the vehicle systems to transition from safe to hazardous states.

UCA Identification:

For each control action, consider:

1. Relevant system states
2. Six UCA guidewords

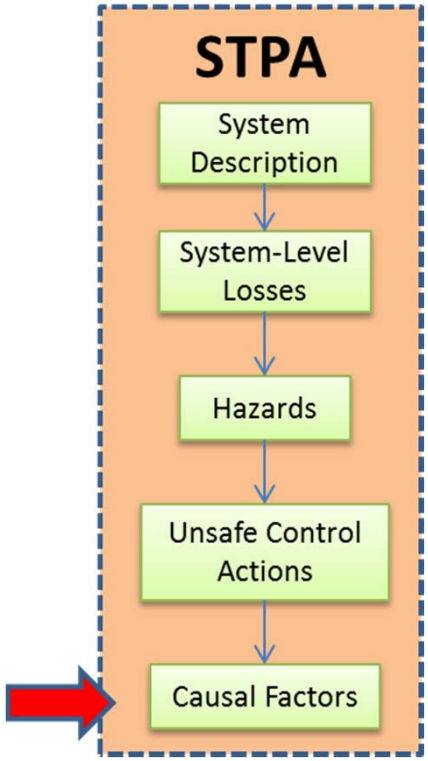




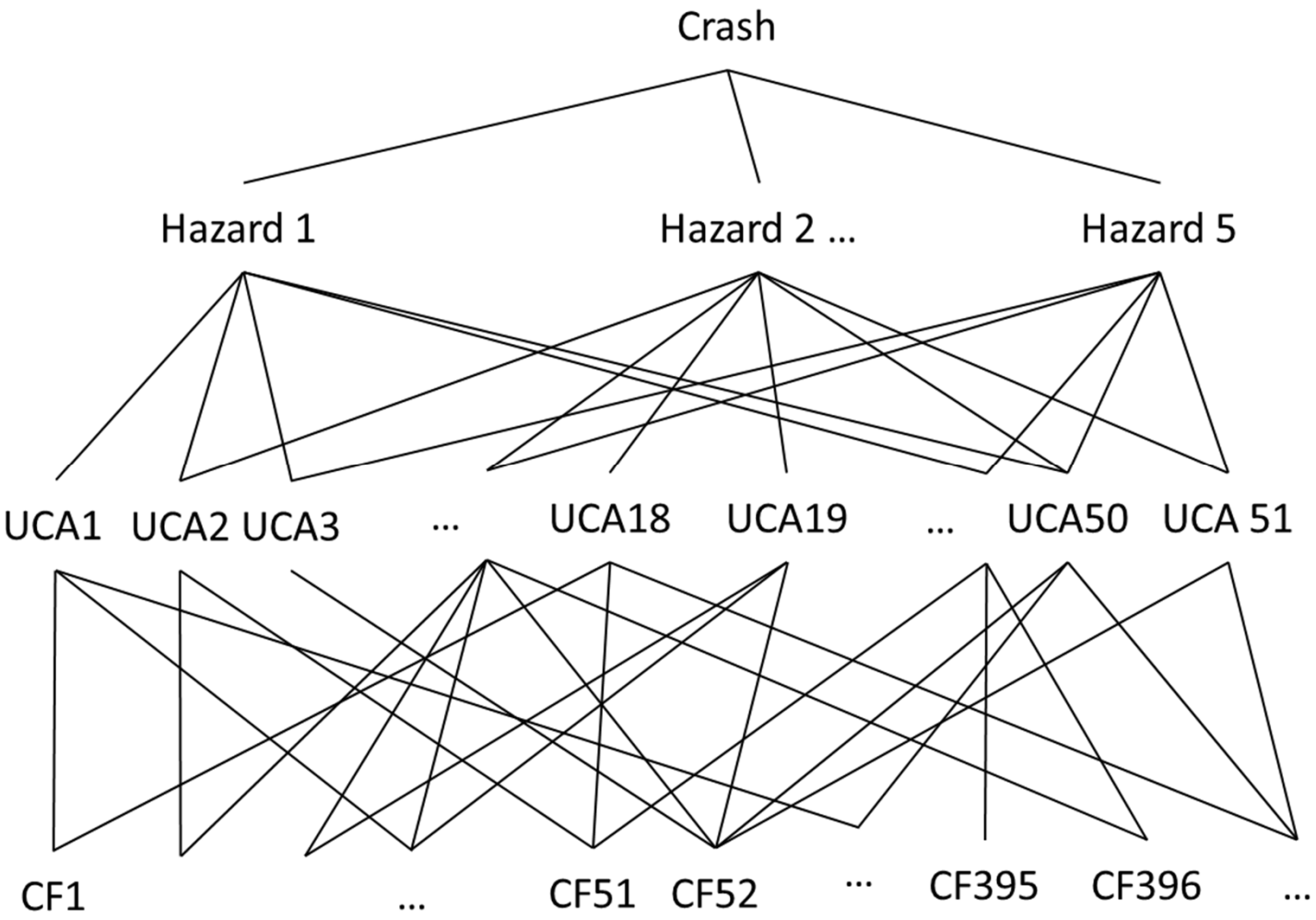
STPA Step 2: Causal Factor Categories

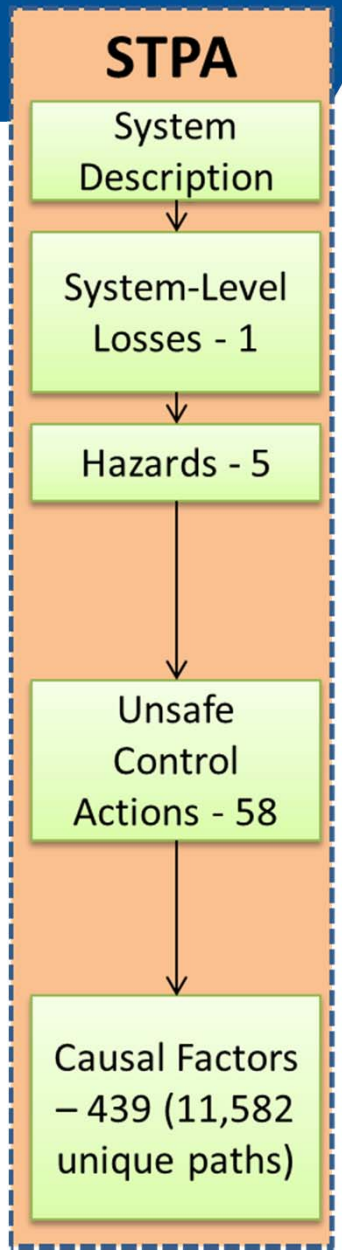
Causal factors (CFs) consider the following aspects of the control systems:

- Controller
- Sensor
- Actuator
- Controlled Process
- Communication links (wiring, connectors, or communication bus)
- Unsafe Interaction with Other Vehicle Systems
- Unsafe Interaction with External Environment

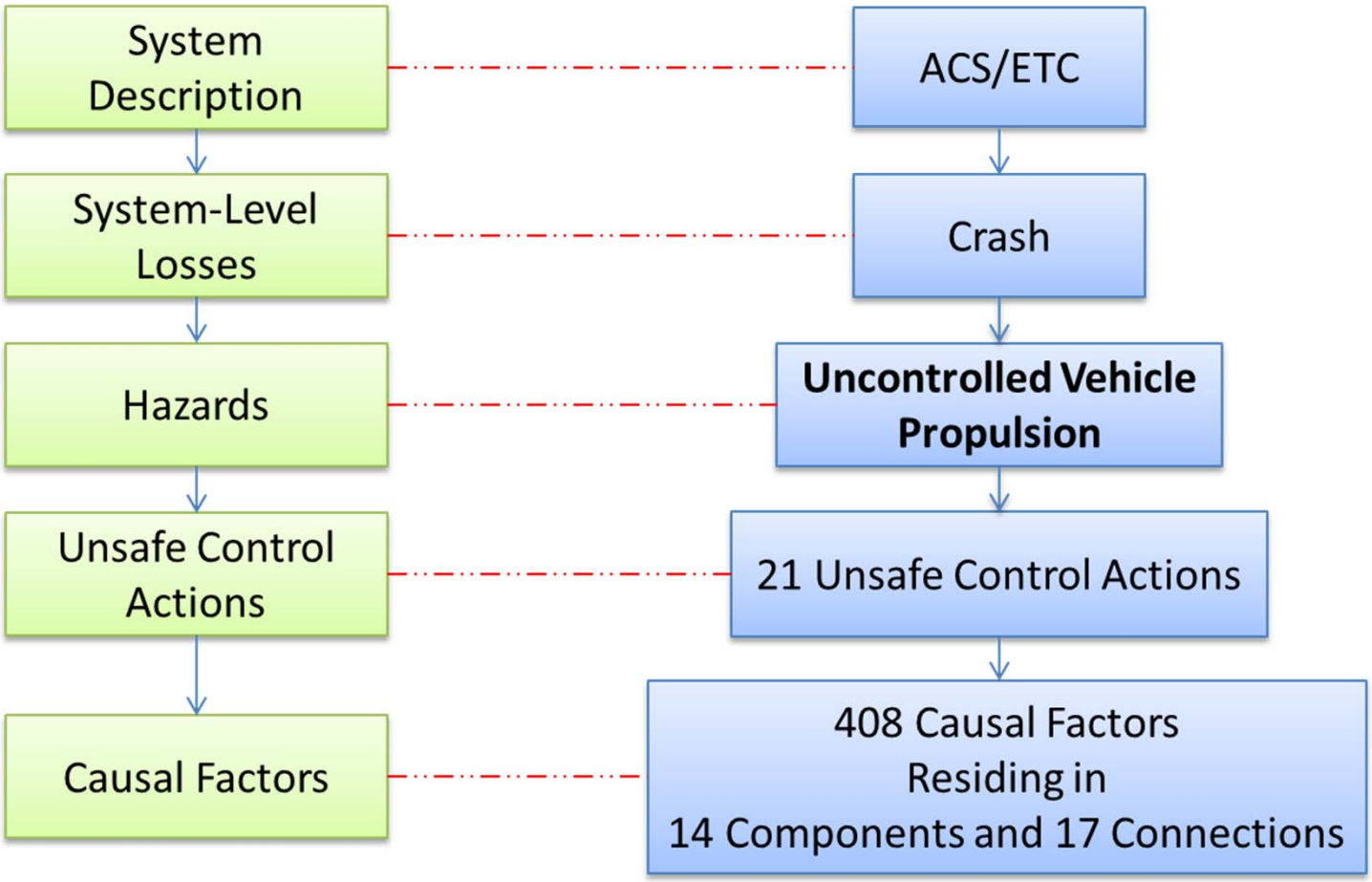


Gasoline ICE ACS/ETC STPA Statistics





Example Results (Preliminary) from the Gasoline ICE ACS/ETC STPA



Example Results (Preliminary) from the Gasoline ICE ACS/ETC STPA (Continued)

Hazard	Uncontrolled Vehicle Propulsion	
Unsafe Control Action Example	The Engine Control Module (ECM) does not issue the *Enter Brake/Throttle Override (BTO) Mode* command when: - driver presses the accelerator pedal, - driver presses the brake pedal, and - vehicle speed is 10 mph or greater.	
Causal Factor Examples	**Component /Connection**	**Causal Factor**
	Engine Control Module	The sequence of pedal application is either not considered or is incorrectly considered in the software logic for entering BTO or Normal mode.
	Accelerator Pedal Position Sensor (APPS)	A hardware failure in the accelerator pedal position sensor could result in an open circuit or an intermittent open circuit. If the signal from the APPS becomes intermittent, this could cause the ECM to think the pedal conflict is removed and exit BTO mode.
	Connection between Brake Pedal Position Sensor and Engine Control Module	Chafing or interference from other vehicle systems could affect the connection between the brake pedal position sensor and ECM (e.g., wiring is cut). This could cause the ECM to receive no signal or an incorrect, intermittent, or delayed signal from the brake pedal position sensor.

Summary

- Research follows the process described in the Concept Phase of the ISO 26262 standard.
- STPA, HAZOP, and FMEA methods are used for comprehensive hazard and safety analyses.
- Results of the hazard and safety analyses are used to generate the functional safety concept and the safety requirements.
- Hazard and safety analyses of the ACS/ETC and ALC control systems are underway.
- Completed the safety analysis for the automotive RESS.

QUESTIONS?

Qi Van Eikema Hommes
Electronics Engineer
Advanced Vehicle Technology Division
Volpe National Transportation Systems Center

(617) 494-2964