Applying STAMP Framework to Analyze Automotive Recalls

Dr. Qi Van Eikema Hommes

March 27, 2014
Presentation Outline

- Research Need
- Analysis Approach
- Data Selection
- Analysis Scope
- Results
- Summary
Research Needs

Safety challenges posed by the proliferation and increasingly-interconnected electronic systems\(^1\):

- Increased amount of complex software that cannot be exhaustively tested
- Highly interactive nature of the electronic control system – more interactions exist among system components, and the outcome may be difficult to anticipate
- Growing importance of human factors consideration in automotive electronic control system design
- Potentially harmful interaction with the external environment including EMI
- Novel and rapidly changing technology

Research Goals

Build a scientific foundation to identify and define automotive electronic control system safety issues:

1. Characterize documented electronic control system safety issues, including the creation of a failure causal factor typology

2. Quantify safety-critical electronic systems safety issues (not ranking or prioritize)

3. Research and develop a new data coding scheme to allow for more efficient data mining for quantification of trends and causal factors
Analysis Approach

• Develop a typology of automotive electronic control system failures based on control system engineering principles
• Populate a database for analysis using historical vehicle failure data
Data Source Selection Process

- **Data Requirements:**
  - Publically available
  - Definitively demonstrates that a safety issue exists

- **Data Considered:**
  - NHTSA Complaint Monitoring and Investigation Databases:
    - Vehicle Owner’s Questionnaire (VOQ)
    - Defect Investigations
    - Motor Vehicle Recalls
  - NHTSA Crash Databases:
    - National Automotive Sampling System (NASS) General Estimates System (GES)
    - Fatality Analysis Reporting System (FARS)

- **Data Selected:**
  - NHTSA Motor Vehicle Recalls
Data Limitations

- Recall data may not be representative of all vehicle failures in the field.
- If observations made from recall statistics were to be generalized, a weighting scheme must be carefully devised.
- Publically available recall documents provide varying amount of technical details, which may cause misinterpretation for data coding.
- Historical trends may not be truly indicative of future problems.
Recall Analysis Scope
Data Scope

- This study concentrates on malfunctions of electronic control systems caused by:
  - Components (including software) not performing manufacturers’ intended functions
  - Unsafe system interactions with other vehicle components
  - Unsafe interactions with the external environment

- Target Data Filtering:
  - Light Vehicles with gross vehicle weight rating less than 10,000 lbs
  - Model Year (MY) 2002-2013
  - Recalls recorded by April 30, 2013

Total Recalls (1,892) ➔ Electronic system related (538) ➔ Target (315)
Electronic Control Systems Considered (Alphabetical Order)

- Active suspension management
- Antilock brake system (ABS)
- Electronic parking brake
- Climate control
- Electronic power steering
- Electronic stability control (ESC)
- Powertrain control
- Engine cooling control
- Exterior lighting
- Hybrid and electric vehicle (HEV) cooling
- HEV electrical
- Ignition key/starter
- Instrument cluster and driver-vehicle interface
- Integrated motor assist
- Power door/window control
- Restraints
- Tire pressure monitoring system (TPMS)
- Traction control
- Transmission control
- Vehicle speed control
- Windshield wiper and washer
Example Recall Analysis

- Campaign Number: 07V178000
- Model Year: 2007
- Component: Air Bags: Frontal: Sensor/Control Module
- Summary: Certain passenger vehicles fail to conform to the requirements of Federal Motor Vehicle Safety Standard No. 208, ‘Occupant Crash Protection.’ The front passenger seat has a sensing system to detect if the seat is occupied. This sensing is programmed to detect if the seat is occupied by a small adult or certain child restraint seats. Placing certain child seats on the front passenger seat is designed to result in the automatic deactivation of the front seat passenger’s air bag.
- Consequence: In some cases, the sensing system may misinterpret a properly seated small adult as one of these specific child seats, resulting in deactivation of the front passenger air bag when the air bag might be beneficial for the adult, increasing the risk of injury in a crash.
- Remedy: Dealers will replace the front passenger seat sensor.

Source: http://safercar.gov
Air Bag Control System

Driver

Air bag status indicator

Passenger air bag on/off indicator light

Air Bag Control Unit (Sensing and Diagnostic Module)

Seatbelt Tension Command

Airbag Deploy Command

Inflator (Ignitor, Diffusor, etc.)

Seatbelt Tensioner

Seatbelt Tension

Explosion and release of the gas

Occupants in Seats in the Vehicle

Vehicle deceleration signal

Deceleration Information

Seat position

Seat Track Position Sensor

Passenger Presence Sensor

Passenger Presence Sensing Module (sensor calibration)

Seat Position

Air bag enable/disable requests

Sensing module fault code

Passenger sensing module on/off command

Sensor signal

Seat Belt Tension Sensor
Example Recall Analysis (Cont.)

- Hazard: Restraint system loss or degradation
- Vehicle Section: Body
- Vehicle System: Restraint System
- Unsafe Control Action: Air bag may not deploy when it should
- Component failure: Failed component is within the air bag control system
- Hardware failure: Electronics/Electrical component
- Causal Factor: Sensor inadequate operation, change over time
- Causal Component: Passenger Presence Sensor
Data Coding

Recalls

Hazard (15)

Potentially Unsafe Control Action

• 47 control actions
• 6 unsafe control action guidewords

Causal Factors (26)

Vehicle

• 4 major sections

Electronic Control System

• 21 electronic control systems
• 18 controller

Failed System Components or Unsafe System Interactions (132)
Vehicle Level Hazards

1. Anti-theft function loss or degradation
2. Braking malfunction
3. Electronic component overheating
4. Impeding driver ability to control vehicle
5. Inadvertent engine start
6. Pinch detection loss or degradation
7. Restraint system malfunction (loss, degradation, or inadvertent deployment)
8. Roadway illumination and vehicle conspicuity loss or degradation
9. Steering loss or degradation
10. Unintended door opening
11. Vehicle inability to accelerate or stalling
12. Vehicle unintended acceleration
13. Vehicle instability
14. Vehicle movement in unexpected direction
15. Windshield visibility loss or degradation

*Note: Bold fonts indicate vehicle motion related hazards*
Unsafe Control Actions

- Provided
  - Not Needed and Hazardous (1)
    - Intensity is incorrect (2)
      - Delivered incorrectly (3)
    - Duration is too long or too short (4)
      - Starting time is too soon or too late (5)
- Needed
- Not Provided
  - But needed to maintain safety (6)
Causal Factors

Controller

1. External control input or information wrong or missing.
2. External disturbances faulty (high, low, disturbance)
3. Power supply faulty (high, low, disturbance)
4. Hazardous interaction with other components in the rest of the vehicle
5. Controller signal ineffective, missing, or delayed:
   a. Hardware open, short, missing, intermittent faulty
   b. Communication bus error
   c. Incorrect connection
6. Controller hardware faulty, change over time
7. Software error (inadequate control algorithm, flaws in creation, modification, or adaptation)
8. Process model or calibration incomplete or incorrect
9. Sensor inadequate operation, change over time
10. Sensor signal inadequate, missing, or delayed:
   a. Hardware open, short, missing, intermittent faulty
   b. Communication bus error
   c. Incorrect connection
11. Actuator to controller signal ineffective, missing, or delayed:
    a. Hardware open, short, missing, intermittent faulty
    b. Communication bus error
    c. Incorrect connection
12. Sensor measurement incorrect or missing
13. Sensor measurement inaccurate
14. Sensor measurement delay
15. Actuator inadequate operation, change over time
16. Hardware faulty
17. Communication bus error
18. Incorrect connection
19. Actuation delivered incorrectly or inadequately
20. Controlled component failure, change over time
21. Input to controlled process missing or wrong
22. Output of controlled process contributes to system hazard
23. Process input supplier inadequate operation, change over time
24. Incorrect connection
25. Incorrect connection
26. Incorrect connection

Adapted and Modified from Leveson 2012
Book Version of the Causal Factors

(1) Control input or external information wrong or missing

Controller
(2) Inadequate Control Algorithm
(3) Process Model inconsistent, incomplete, or incorrect
(k) Controller hardware faulty

Sensor
(a) Inadequate or missing feedback
(b) Feedback delays

Actuator
(o) Inappropriate, ineffective, or missing control action

(6) Inadequate operation
(i) Delayed operation

Controlled Process
(5) Component failures, change over time

(h) Process input missing or wrong
(g) Unidentified or out-of-range disturbance
(f) Process output contributes to system hazard
Component Failure and Unsafe System Interactions

1. Component Failure
   - Hardware
     - Inside the Electronic Control System
     - Outside the Electronic Control System
   - Software
     - Inside the Electronic Control System
     - Outside the Electronic Control System

2. Unsafe Interaction with Other Vehicle Systems
   - Hardware-Hardware
   - Hardware-Software

3. Interaction with External Environment
Preliminary Data Analysis Results
Frequency of Hazards

- Restraint System Malfunction: 88
- Vehicle Inability to Accelerate or Stalling: 72
- Vehicle Instability: 60
- Roadway Illumination and Vehicle Conspicuity Loss or Degradation: 39
- Windshield Visibility Loss or Degradation: 23
- Electronic Component Overheating: 14
- Unintended Acceleration: 12
- Vehicle Movement in Unexpected Direction: 9
- Impeding Driver Ability to Control Vehicle: 8
- Braking Malfunction: 7
- Steering Loss or Degradation: 5
- Pinch Detection Loss or Degradation: 5
- Anti-Theft Function Loss or Degradation: 4
- Unintended Opening of Door: 2
- Inadvertent Engine Start: 1
Frequency of Unsafe Control Actions

- Control action is not provided when needed for safety: 197
- Control action is provided when it is not needed and unsafe: 74
- Control action needed for safety is provided but is incorrectly executed: 34
- Control action needed for safety is provided correctly,...: 28
- Not caused by unsafe control action: 13
- Control action is provided but duration is too long or too short: 11
- Control action is provided but starting time is too soon or too late: 7

Number of Recall Campaigns
Frequency of Causal Factors

- Software error (inadequate control algorithm, flaws in creation, modification, or adaptation) - 2.6 million
- Sensor inadequate operation, change over time - 10.5 million
- Actuator inadequate operation, change over time - 4.8 million
- External Disturbance - 4 million
- Controller hardware faulty, change over time - 4.2 million
- All Other Causal Factors - 11.7 million

The numbers to the right of the bar represent the number of vehicles recalled in millions.
Summary

Built a scientific foundation to define and quantify automotive electronic control system safety issues:

1. Based on a top-down Systems Engineering approach and control system principles
2. Created a new failure causal factor typology and data coding scheme
3. Quantified automotive electronic systems safety issues using the new data coding scheme
4. Constructed a coded database with respect to automotive electronic control system safety:
   - Contains a comprehensive list of variables that classifies causes of safety problems associated with automotive electronic control systems
   - Easy to adapt to new safety-critical motor vehicle system technologies and future recalls
   - Enables us to:
     - Assess the overall state of electronic control system safety and identify existing and potential safety problems
     - Provide a basis for regulatory and consumer initiatives, evaluation of vehicle safety systems and designs, and focused cost-benefit analyses
     - Answer questions from researchers, private industry, students, public sector, and general public
     - Evaluate the effectiveness of motor vehicle and traffic safety program standards
Questions?

Dr. Qi Van Eikema Hommes
Qi.vaneikemahommes@dot.gov