System Approach to Prevent Quality and Safety Problems in Modern Automobiles

Dr. Qi Van Eikema Hommes

May 14, 2012
Presentation Outline

• Characteristics of today’s automobiles
• Our customary design approach
  – Decomposition
  – Industry standard – ISO 26262
• System Theoretic Approach
  – Adaptive Cruise Control case study
Automobiles Were Mechanical Systems

Henry Ford in his first car, the Quadricycle, built in 1896
Today’s Automobiles are Complex Electronic Systems

Premier automobiles have ~60 microprocessors onboard.
Let The Robot Drive

Wired, Feb 2012, http://www.wired.com/magazine/2012/01/ff_autonomouscars/all/1
Automotive Systems Today and Tomorrow

- Cyber Physical Systems - complex embedded devices networked to control physical hardware components.
- Software intensive.
- Automating many human tasks.
- The development teams are multidisciplinary and globally distributed.
Lines of Codes Comparison

- F-22 Raptor (US Air Force Frontline Jet Fighter): 1.7 Million Lines of Codes
- F-35 Joint Strike Fighter (still in development phase): 5.7 Million Lines of Codes
- Boeing 787 Dreamliner: 6.5 Million Lines of Codes
- Today's Premium Class Automobile: 100 Million Lines of Codes
- Automotive Forecast by Frost & Sullivan: 300 Million Lines of Codes

Charette 2009
Quality Problem With no Component Failure

- Trouble-Not-Identified Engine Control Module warranty problem.
- No component failure was found.
- Insufficient resource to conduct exhaustive bottom-up testing, after the product was already released to market.
- Many such quality problems are never resolved.
Toyota Unintended Acceleration

**The Detroit News**

April 6, 2010

Toyota faces $16.4M fine for hiding safety defect

Proposed penalty is largest ever sought by NHTSA officials

**NASA to help probe unintended auto acceleration**

March 30, 2010

Washington -- Federal safety regulators are seeking to fine Toyota Motor Corp. $16.4 million -- the largest ever penalty against an automaker -- for failing to disclose problems with sticky accelerator pedals in a timely manner.

Washington -- The U.S. Transportation Department will launch two major investigations to discover whether vehicle electronics or electromagnetic interference are to blame for unintended vehicle acceleration incidents.
Presentation Outline

• Characteristics of today’s automobiles
• Our customary design approach
  – Decomposition
  – Industry standard – ISO 26262
• System Theoretic Approach
  – Adaptive Cruise Control case study
Traditional Engineering Design Method
Pahl and Beitz 2007

Design Catalog: Component design solution look up table
Typical Decomposition Scheme

• **Physical**: usually stated as systems, subsystems, subassemblies, parts
  – Car systems and subsystems include seats, engine, suspension, steering

• **Organizational**: Usually stated as divisions, departments, groups, etc.
  – Powertrain department, Research and Development division, etc.

• **Process**: usually stated as phases of the product development process.
  – Concept development, detailed design, etc., each with tasks and subtasks.
The Effects of Decomposition

• Quality and safety = component failure prevention
  • Failure: Not performing intended function

• Quality and Safety Engineering = Reliability Engineering

• Component failures are random hardware failures
  – Not useful for complex software system
  – Not useful for social systems

• The reality: many unresolved quality and safety problems.
An Example of System Interactive Complexity: The Powertrain Control Software System

- 1 production-level software
- 117 software modules (red dots)
- 1423 interactions (black lines)
- 39 such production software releases per year
- <2 weeks per release

Hommes, DETC2008-DTM-49140
We Rely Heavily on Experts’ Tacit Knowledge to Handle System Interactions and Integration

Based on three industry case studies.
The graph shows a general trend and is not a comparison of the companies.
Causes of Undesirable System States

• Component failure
  – FMEA
  – FTA
  – Reliability Engineering

• Undesirable component interaction
  – Acerbated by introduction of new technologies, design changes, parts reuse, growing amount of computers and software.
  – Emergent behavior of the system that reliability engineering alone cannot address.
  – Systemic causes within the social context (engineering development, regulation, policy makers)

• Hazard analysis methods need to include both component failures and undesirable component interactions.
Presentation Outline

• Characteristics of today’s automobiles

• Our customary design approach
  – Decomposition
  – Industry standard – ISO 26262

• System Theoretic Approach
  – Adaptive Cruise Control case study
ISO 26262 Functional Safety for Road Vehicle

• The first comprehensive standard that addresses safety related automotive systems comprised of electrical, electronic, and software elements that provide safety-related functions.
• Adaptation of IEC 61508 to road vehicles
• Influenced by ISO 16949 Quality Management System

For detailed assessment, please refer to Van Eikema Hommes, SAE 2012-01-0025
## General Structure of ISO 26262

### 1. Vocabulary
- 2-5 Overall safety management
- 2-6 Safety management during item development
- 2-7 Safety management after release for production

### 2. Management of functional safety
- 3. Concept phase
  - 3-5 Item definition
  - 3-6 Initiation of the safety lifecycle
  - 3-7 Hazard analysis and risk assessment
  - 3-8 Functional safety concept
- 4. Product development: system level
  - 4-5 Initiation of product development at the system level
  - 4-6 Specification of the technical safety requirements
  - 4-7 System design
  - 4-8 Item integration and testing
  - 4-9 Safety validation
  - 4-10 Functional safety assessment
  - 4-11 Release for production
- 5. Product development: hardware level
  - 5-5 Initiation of product development at the hardware level
  - 5-6 Specification of hardware safety requirements
  - 5-7 Hardware design
  - 5-8 Hardware architectural metrics
  - 5-9 Evaluation of violation of the safety goal due to random HW failures
  - 5-10 Hardware integration and testing
- 6. Product development: software level
  - 6-5 Initiation of product development at the software level
  - 6-6 Specification of software safety requirements
  - 6-7 Software architectural design
  - 6-8 Software unit design and implementation
  - 6-9 Software unit testing
  - 6-10 Software integration and testing
  - 6-11 Software verification

### 3. Core processes
- 8. Supporting processes
  - 8-5 Interfaces within distributed developments
  - 8-6 Overall management of safety requirements
  - 8-7 Configuration management
  - 8-8 Change management
  - 8-9 Verification
  - 8-10 Documentation
  - 8-11 Qualification of software tools
  - 8-12 Qualification of software components
  - 8-13 Qualification of hardware components
  - 8-14 Proven in use argument

### 4. ASIL-oriented and safety-oriented analyses
- 9-5 Requirements decomposition with respect to ASIL tailoring
- 9-6 Criteria for coexistence of
- 9-7 Analysis of dependent failures
- 9-8 Safety analyses

### 5. Support
- 10. (Informative) Guidelines on ISO 26262

---

©5/14/12
Qi D. Van Eikema Hommes
Source: ISO 26262
Strengths

• Emphasizes safety management and safety culture
• Prescribes a systems engineering process
• Departures from safety as an after-thought:
  – IEC 61508: safety function (safety is an add-on)
  – ISO 26262: provides the framework and vocabulary for hazard elimination in the first place
    • Systems engineering framework
    • Safety measure vs. safety mechanisms
Suggestions for Improvements

• Safety measure is not clearly explained in the document, while Safety Mechanism is explained in detail throughout the document.

• The standard may want to add a section in Part 1 to further clarify the departure from IEC 61508’s design philosophy.
Reliability Engineering based Hazard Analysis Methods and Safety Assurance Approaches

• **Hardware Architecture Metrics**--Based on random failure of components.
• **Failure Modes and Effects Analysis (FMEA)**
• **Fault Tree Analysis (FTA)**
• **Safety Case Approach**
  – Confirmation bias
  – The use of Quantitative Risk Assessment
Software Safety

• Follows software system engineering process
• Promotes good software architecture practices
• On Par with other software safety standards such as DO-178

Comments:
• Unlike hardware, software does not fail.
• Software faults are due to design errors, but the standard does not offer a way to identify design errors that can cause hazard.
• Good systems engineering process and software architecture design are necessary but not sufficient to ensure system safety.
Presentation Outline

- Characteristics of today’s automobiles
- Our customary design approach
  - Decomposition
  - Industry standard – ISO 26262
- System Theoretic Approach
  - Adaptive Cruise Control case study
System Theory

- Focuses on the concept of an irreducible whole.
- **Hierarchy and Emergence:**
  - The world is organized hierarchically.
  - There are properties (emergent properties) at the higher level of the system that are meaningless to discuss at the lower level.
  - Higher level emergent properties impose constraints on the lower level components.
- **Controls and Communication:**
  - Control imposes constraints from higher level of the system hierarchy onto lower levels.
  - All Control process depends on communication—the flow of information.
System Theoretic Accident Model and Process (STAMP)

• Accidents are not caused just by random component failures.
• Accidents are caused by unsafe control actions from the higher level controllers onto the lower level components.
• Can analyze both component failures and undesirable system interactions.
Generic Control Structure in STAMP Model

Leveson 2012
System Theoretic Process Analysis (STPA)

- A systems engineering approach to decompose top level safety goals.
- The outcome is a list of design requirements on the lower level components that will prevent the top level accident.
- STPA provides a top-down guided approach to decompose high level safety goals to components level design requirements.
ADAPTIVE CRUISE CONTROL

1 Vehicle cruise control set at 70 mph
2 Radar detects slower vehicle ahead, reduces speed to return vehicle to a pre-set following distance
3 Cruise control adjusts to the lead vehicle’s speed and resets to the original speed if traffic clears

Source: media.ford.com
Accident, Hazard

- **Accident**: vehicle occupants are injured while ACC is engaged.
- **Hazards**:
  - H1: ACC did not maintain a safe distance from the object in the front, resulting in collision.
  - H2: ACC slows down the vehicle too abruptly, and vehicle is rear-ended.
System Safety Constraints and Requirements

- **Design constraints:**
  - ACC should not let the vehicle gets in contact with the object ahead.
  - ACC should not brake too abruptly.

- **Design requirements:**
  - ACC shall maintain a TBD amount of distance between the vehicle and the object in front when engaged.
  - ACC shall limit vehicle deceleration to no more than TBD m/s^2.
Hierarchical Control Structure

Operator

Tactile input

Visual Feedback

Tactile input

Brake Pedal

Braking Signal

Wheel Speed

Brake Control Module

Braking Signal

Braking Status
Vehicle Speed

ACC Module

Distance

Target Vehicle Speed

Powertrain Control Module

Acceleration Signal

Throttle opening

Electronic Throttle Body

Throttle Position

Vehicle

Air

Radar

Lead Vehicle

©5/14/12

Qi D. Van Eikema Hommes

32
Reformatted Control Loop

Control Action: Brake
Signal from ACC to BCM
# STPA Step 1: Unsafe Control Actions

<table>
<thead>
<tr>
<th>Control Action</th>
<th>Not Providing Causes Hazard</th>
<th>Providing Causes Hazard</th>
<th>Wrong Timing or Order Causes Hazard</th>
<th>Stopped too Soon or Applied Too Long</th>
</tr>
</thead>
<tbody>
<tr>
<td>Brake Signal from ACC to BCM</td>
<td>Vehicle does not brake when the distance to the lead vehicle is less than the value set by the operator. (H1)</td>
<td>Commanded deceleration amount is too small when the vehicle is too close to the object in the front. (H1)</td>
<td>Braking is commanded too late when the distance to the lead vehicle is too close. (H1)</td>
<td>Braking stops before the safety distance between the vehicles are reached. (H1)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Braking is commented when the distance to the lead vehicle is larger than the set value. (H2)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Braking is too fast/harsh when the distance to the lead vehicle is less than the set value. (H2)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
STPA Step 2: Causal Analysis with Guidewords

Controller

1. Control input or external information wrong or missing

2. Inadequate Control Algorithm
   (Flaws in creation, process changes, incorrect modification or adaptation)

3. Process Model inconsistent, incomplete, or incorrect

4. Inadequate operation

Actuator

Inappropriate, ineffective or missing control action

Sensor

Inadequate or missing feedback

Feedback Delays

Inadequate or no information provided

Measurement inaccuracies

Feedback delays

Controlled Process

4. Component failures Changes over time

Process input missing or wrong

Unidentified or out-of-range disturbance

Process output contributes to system hazard

Leveson 2012
Causal Analysis Results

Unsafe Control Action:
Vehicle does not brake when the distance to the object in front is less than preset value.
Unsafe Control Action:
Vehicle does not brake when the distance to the object in front is less than preset value.

Delayed Operation
Causal Analysis Results (3)

Unsafe Control Action:
Vehicle does not brake when the distance to the object in front is less than preset value.

- Misalignment of brake shoes/pads.
- Missing fluid pressure for hydraulic lines.
- No current/voltage to actuator.
Unsafe Control Action: Vehicle does not brake when the distance to the object in front is less than preset value.
Causal Analysis Results (5)

Unsafe Control Action:
Vehicle does not brake when the distance to the object in front is less than preset value.

- Dirt accumulation on wheel rotation sensor.
- Wire disconnection.
- Communication bus faults, overload, message priority.
Assess the Effectiveness of STPA

• The outcome of STPA was a list of component design requirements that will ensure top level safety goal.

• Compare with actual industry design specifications.
  – Unable to do so because of proprietary nature of the design specifications.
Assess STPA (2)

• Compared with ISO 22179 and SAE J2399.
  – Many more detailed requirements than what is in the standards.
  – Industry standards are the lowest common denominators among the manufacturers.
  – Can only compare with categories of requirements.

• Compared with actual implementation in production vehicles.
  – Warning signals among manufacturers
  – Warnings in driver’s manual
Categories of Requirements Missing in Industry Standards

• Driver control authority vs. computer automation authority
  – The importance of vehicle state feedback information (warning lights/sounds/icons) for driver
  – Driver mental model inconsistency with vehicle state (complacency and distracted driving)

• Sensor and actuator
  – Hardware quality
  – Degradation
Categories of Requirements Missing in Industry Standards (2)

• Communication bus
  – Delays
  – Signal priority

• Controls software errors
  – Delay in processing inputs
  – Parameter calibration errors
  – Control software algorithm process model
  – Software handling of signal priority

• Service and maintenance requirements
Comparison with Implementation

1. Significant difference in the implementation of warning messages and signals among OEM’s and across models.

Example: ACC Malfunction Lights (Credit: Zoepf)

- Porsche
- Toyota
- Volvo
- Nissan

2. Leaving a lot of the limitations of ACC in the drivers’ manual.

- NISSAN INFINITI EX 2010, 21 pages (ACC feature), 16 warnings and 1 caution.
- Ford Lincoln MKX 2010, 7 pages (ACC feature), 10 warnings.
ACC Cast Study Summary

• This was my first attempt to apply STPA to a modern automotive electronics feature.
• The method works.
• The analysis identified many more safety critical requirements than what is identified in the industry standards.
• STPA can be a very powerful method to identify safety critical design requirements, and prevent accidents in the first place.
• Industry collaboration will further improve our understanding of the effectiveness of the method, and how to integrate it with the current product development process.
Summary

• Automotive systems have changed—more complex, software intensive, more automation.

• Reductionist approach is no longer adequate.

• ISO 26262 is our latest effort to address our new challenges. It can be improved by incorporating more systems approach.

• STPA based is a promising direction for improving the quality and safety of automotive electronic systems.
Next Step: Research Partnership on Automotive Functional Safety

• Industry – Government – Academia Collaboration

• Funded research projects
  – Develop a scientific framework for automotive electronics safety engineering.
  – Develop a non-proprietary test bed that reflect the real world challenges.
  – Prepare future engineers for the new kinds of systems we are designing.

• Shared learning among members to
  – Improve design for safety
  – Improve industry standards
  – Support safety regulation
New Academic Program

• MIT new Master’s degree program with a concentration on system approach to safety:
References


Thank you!

Questions?