Safety Analysis of Heavy-Duty Truck Platooning Systems

Doug Pape
Battelle
Safety Analysis of Heavy-Duty Truck Platooning Systems

Battelle is conducting this research for NHTSA

- List of Current and Future Products
- Hazard Analysis and Risk Assessment
- Safety Analysis

Study Completion: Summer 2020.
A Sampling of Platooning Projects

Volvo

Peloton

Texas A&M Transportation Institute

TARDEC
Safety Analysis of Heavy-Duty Truck Platooning Systems

List of Current and Future Products

Hazard Analysis and Risk Assessment

Safety Analysis
Hazards

An event that poses danger to people, the system, or the environment
Caused by human error, hardware failure, or software defect (usually)
May be caused by limits of system design (scenario not anticipated)
Identifying Hazards

Preliminary Hazard Analysis (PHA)
More formalized than brainstorming

Decompose the design to subsystems or blocks
- Identify failures of the function of each block
- Identify failures of the interfaces
- Identify failures from the environment and from human factors

Then characterize the risk of every hazard.
Risk Characterization

<table>
<thead>
<tr>
<th>Hazard Severity</th>
<th>S3</th>
<th>S2</th>
<th>S1</th>
<th>S0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Life-threatening injuries (survival uncertain), fatal injuries</td>
<td>E4</td>
<td>E3</td>
<td>E2</td>
<td>E1</td>
</tr>
<tr>
<td>Severe and life-threatening injuries (survival probable)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Light and moderate injuries</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>No injuries</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Hazard Probability

- High probability
- Medium probability
- Low probability
- Very low probability
- Incredible
ISO 26262 adds a third dimension—Controllability

<table>
<thead>
<tr>
<th>Severity</th>
<th>Exposure</th>
<th>Controllability</th>
</tr>
</thead>
<tbody>
<tr>
<td>S1</td>
<td></td>
<td>C1</td>
</tr>
<tr>
<td>E1</td>
<td>QM</td>
<td>QM</td>
</tr>
<tr>
<td>E2</td>
<td>QM</td>
<td>QM</td>
</tr>
<tr>
<td>E3</td>
<td>QM</td>
<td>QM</td>
</tr>
<tr>
<td>E4</td>
<td>QM</td>
<td>A</td>
</tr>
<tr>
<td>S2</td>
<td></td>
<td>C1</td>
</tr>
<tr>
<td>E1</td>
<td>QM</td>
<td>QM</td>
</tr>
<tr>
<td>E2</td>
<td>QM</td>
<td>QM</td>
</tr>
<tr>
<td>E3</td>
<td>QM</td>
<td>A</td>
</tr>
<tr>
<td>E4</td>
<td>A</td>
<td>B</td>
</tr>
<tr>
<td>S3</td>
<td></td>
<td>C1</td>
</tr>
<tr>
<td>E1</td>
<td>QM</td>
<td>QM</td>
</tr>
<tr>
<td>E2</td>
<td>QM</td>
<td>A</td>
</tr>
<tr>
<td>E3</td>
<td>A</td>
<td>B</td>
</tr>
<tr>
<td>E4</td>
<td>B</td>
<td>C</td>
</tr>
</tbody>
</table>
Classes of Hazards We Are Considering

- Communication failures (message lost, delayed, corrupted)
- Component failures (hardware failures, software errors)
- Vehicle factors (brake failures, differences in brake rates)
- Environmental factors (weather, other traffic)
- Driver issues (lack of training, acclimatization with the system)
- Human factors (reliance, fatigue, workload, fumes from close following, trust in the other driver, standardization across brands)
Safety Analysis of Heavy-Duty Truck Platooning Systems

List of Current and Future Products

Hazard Analysis and Risk Assessment

Safety Analysis
Common Safety Analysis Techniques

Failure Modes & Effects Analysis
FMEA
Bottom → Up

Fault Tree Analysis
FTA
Top → Down
Failure Modes & Effects Analysis

Bottom Up
A Failure Modes & Effects Analysis determines how a system might fail and the likely effects of particular modes of a failure.
Failure Modes & Effects Analysis

What can go wrong with the input?
Failure Modes & Effects Analysis

What can go wrong with the input?

What is the effect on the output?
Failure Modes & Effects Analysis

What can go wrong with the input?

What is the effect on the output?

How bad?
Failure Modes & Effects Analysis

- What can go wrong with the input?
- What is the effect on the output?
- What are the causes?
- How bad?
Failure Modes & Effects Analysis

What can go wrong with the input?

What is the effect on the output?

What are the causes?

How bad?

How often?

What can be done?
Fault Tree Analysis (FTA)

**Top Down**
A Fault Tree Analysis is

a deductive analytical technique

where an undesirable state is specified.

FTA demonstrates how resistant a system is to initiating faults.

FTA of complex systems is labor intensive

but beneficial.
Top-Down Approach

Safety Analysis of Heavy-Duty Truck Platooning Systems

- Truck Crashes
  - Gate 2
    - Radar Fails
      - Event 1
    - Human Error
      - Event 2
    - Brakes Fail
      - Gate 3
Top-Down Approach

Safety Analysis of Heavy-Duty Truck Platooning Systems
Human Factors

Analysis Techniques
• Task analysis
• Workload assessment
• Activity sequence diagram

Possible Faults
• Distraction or boredom
• Confusing message
Questions

Contact Information:

Doug Pape
pape@battelle.org

NHTSA Program Lead:
Alrik Svenson
Alrik.Svenson@dot.gov