A GENERIC FRAMEWORK FOR HAZARD ANALYSIS OF AUTOMATED VEHICLES IN TRANSIT SERVICE –

PROPOSED TRB, FEDERAL AGENCY AND ITS / AUTOMOTIVE INDUSTRY COLLABORATION

J. Sam Lott,
Kimley-Horn and Associates, Inc.

Shared Mobility and Transit Breakout Session
TRB Second Annual Workshop on Road Vehicle Automation
A GENERIC FRAMEWORK FOR HAZARD ANALYSIS OF AUTOMATED VEHICLES IN TRANSIT SERVICE –

PROPOSED TRB, FEDERAL AGENCY AND ITS / AUTOMOTIVE INDUSTRY COLLABORATION

J. Sam Lott, Kimley-Horn and Associates, Inc.

Shared Mobility and Transit Breakout Session

TRB Second Annual Workshop on Road Vehicle Automation
Content

Breakout Session Presentation
• Reasons Why a Generic Hazards Analysis Initiative is Needed
• Proposed Approach of a Generic Hazard Analysis for Automated Vehicle Deployment

Supplemental Information
• ATS/APM Industry Model: The Safety Standards Development Process
• IEC Approach to the Generic Hazard Analysis of Automated Transit Systems
REASONS WHY A GENERIC HAZARDS ANALYSIS INITIATIVE IS NEEDED

Benefits to R&D, Industry Suppliers/Integrators/Operators, and Transportation Agencies
Benefits to the R&D Process

- Common Understanding/Definition of Hazards, Triggers and Means to Provide Safeguards for:
  - Developers/suppliers of automated vehicles (AV)
  - Developers / suppliers of transit supervisory systems, ITS equipment designers, and ATMS signaling/supervisory systems
  - Participation of roadway operators: State DOTs and USDOT

- Mitigation of Risk of Expensive Redesign to Comply with Eventual New Standards

- Early Coordination of Communications Interfaces Between AV and Wayside ITS/ATMS Systems
Benefits to the Automotive Industry, ITS/ATMS Suppliers and Integrators, and Roadway Facility Operators

- Lower Risk of User Confusion Due to Different Production Designs Between Vehicle Manufacturers
  - AV Functional Controls
  - Safety Provisions

- Risk Mitigation of Expensive Redesign to Comply with Eventual New AV Standards

- Faster AV Industry Progress Toward Deployment of Managed Facilities Providing High Speed/High Capacity Operations
Benefits to Agencies Responsible for Roadway Design and Operational Safety

- Federal/State Safety Oversight Regulators Fully Involved in the Definition of AV Functional/Safety Requirements
- Provision of AV Technology to Roadway Users in a Suitably Controlled Process that Ensures
  - Reasonable Uniformity of AV Functions
  - Man/Machine Interfaces
- Informed and Progressive Deployment Allowing Policy Makers, Legislators and Insurers to Keep Pace with Advances in AV Technology
PROPOSED APPROACH OF A GENERIC HAZARD ANALYSIS FOR AUTOMATED VEHICLE DEPLOYMENT

Adaptation of the IEC Approach to the Hazard Analysis of Fully Automated Transit Guideway Systems
ATS/APM Industry Standards Provide a Model Approach for AV Safety Requirements

- Consensus Standards Managed under ASCE and IEC Committee Process
  - Automated People Mover Standards – ASCE 21
  - Automated Urban Guided Transport Safety Requirements – IEC 62267

- Over 20 years of accumulative work through a collaborative process: system/ equipment suppliers, system integrators/operators and safety regulators
### IEC Worksheets Examples Applicable to AV

#### Defining the Hazard:

**Hazard / Cause / Trigger / Accident (Effect)**

<table>
<thead>
<tr>
<th>Case N°</th>
<th>Hazard</th>
<th>Cause</th>
<th>Trigger</th>
<th>Accident (Effect)</th>
<th>Show ALL Safeguards</th>
<th>Can the action or measure compensate for less staff in DTO compared to STO?</th>
<th>Can the action or measure compensate for no staff in UTO?</th>
<th>Remark</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.1</td>
<td><strong>Obstacle from outside the system</strong></td>
<td><strong>Guideways in tunnel:</strong> elements from outside protrude into the clearance of guideway e.g. drill</td>
<td><strong>Train is approaching</strong></td>
<td><strong>Collision with obstacle, person might be injured e.g. derailment, collision, destroying of the carbody</strong></td>
<td><strong>1. External rules</strong></td>
<td><strong>Out of scope of our standard</strong></td>
<td><strong>Out of scope of our standard</strong></td>
<td>Procedures if work is in progress near the tunnel.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td><strong>Guideways above ground:</strong> element from outside the system has fallen on the track e.g. tree, crane, car (vandalism included)</td>
<td><strong>Train is approaching</strong></td>
<td><strong>Collision with obstacle, person might be injured e.g. derailment, collision, destroying of the carbody</strong></td>
<td><strong>2. Rules for checking guideway clearance</strong></td>
<td><strong>Yes</strong></td>
<td><strong>Yes</strong></td>
<td>Protection ride if the clearance is free in the morning or after situations which may produce a hazard (e.g. storms) Combination with on board obstacle detection device necessary.</td>
<td></td>
</tr>
</tbody>
</table>

#### Assessing the Response/Mitigation:

**Safeguard / Action Compensated for By Driver Intervention? / Action Satisfactorily Compensated for W/O Driver?**
Categorization Levels of Automation for Progressive Development of AV-HA

• Transit Guideway Operations
  • Begin with the application/adaptation of IEC Hazards Analysis Table

• Controlled Environment Operations
  • Expand HA for transit and shared-ride AV applications in non-guideway environments

• Open Road Operations
  • Advance the Generic HA to cover non-connected, fully autonomous vehicle operations within unsupervised roadway environments
Transit Guideway Operations

Begin with the application/adaptation of IEC Hazards Analysis Table from IEC 62267-2

- Address both AV On-board and Supervisory Control Systems

- Include appropriate provisions for:
  - Off-line stations
  - Platooning of transit vehicles
  - Transition of AV to/from manually operations when entering/leaving guideway
Controlled Environment Operations

Expand HA for transit and shared-ride AV applications in appropriately “controlled” environments, such as:

- **Campus Environment** for low speed AV operating conditions with provisions for mixed operations among non-AVs, peds and bicycles

- **Managed Lane Facility** for high speed, high capacity operations with connected AV and advisory ATMS
Open Road Operations

Advance the Generic Hazard Analysis to cover non-connected, fully autonomous vehicle operations on common streets/arterials and highways/freeways

• Mixed traffic flows under both low and high speed operation that includes non-automated vehicles

• Operating environments with no ITS/ATMS advisory systems, or connectivity between AVs

• Rural and urban settings with pedestrian and bicycle mixed flow among AVs
Conclusions

- ATS/APM Consensus Standards Provide a Model for AV Safety Requirements
- IEC Generic Hazard Analysis Provides a Starting Point
- Propose Approach Follows a Phased Process for Applying AV Hazard Analysis
  - Start with Transit Guidewey Operations
  - Advance to Controlled Environment Operations Allowing First Generation AVs to Reach Deployment on the Public Roadway System
  - Reach Ultimate Stage of Deployment with Open Road Operations by Fully Autonomous Vehicles in Mixed Flow
A GENERIC FRAMEWORK FOR HAZARD ANALYSIS OF AUTOMATED VEHICLES IN TRANSIT SERVICE –

PROPOSED TRB, FEDERAL AGENCY AND ITS / AUTOMOTIVE INDUSTRY COLLABORATION

QUESTIONS?
SUPPLEMENTAL INFORMATION

ATS/APM INDUSTRY MODEL: THE SAFETY STANDARDS DEVELOPMENT PROCESS

Functional/Safety Standards for the Automated Guideway Transport/ APM Industry
ATS/APM Industry Standards

• Consensus Standard Managed under ASCE Committee Process

• Collaborative Development of Document Content Based on Industry Experience

• Representation from Various User, Supplier and Regulator Interests

• Process Yields Industry Benchmarks Defining Procurement/Regulatory Safety Requirements
ASCE Automated People Mover Standards – ASCE 21

ASCE Committee has worked for over 20 years on this standard

• **Part 1** – Dependability, Safety, ATC and Comm.

• **Part 2** – Vehicles, Propulsion/Braking

• **Part 3** – Electrical, Stations and Guideways

• **Part 4** – System Test, O&M, and Operations

*Next Release to Merge All Parts into Single Standard Document*
Spectrum of APM Technology Addressed in ASCE - 21

- **Traditional AGT – 75-150 Passenger Vehicles**
  - Commonly applied in American Airports
  - Ideal for Urban District Circulator Systems

- **Medium Size APM – 15 Passenger Vehicle**
  - A few applications as District/Campus Circulator
  - Fixed Route or Demand Responsive

- **Small Size ATN/PRT – 4 to 6 Passenger Vehicle**
  - Extension of the pedestrian realm, with a few applications as District/Airport Circulator
  - Demand-responsive service with off-line stations
ASCE–21 APM Technology Spectrum

Miami Metromover – Downtown District Circulator

Masdar City – Urban District Circulator

New York JFK AirTrain – Rail Station to Airport Connector

Toronto Pearson Intl. Airport – District Circulator
IEC Automated Urban Guided Transport Safety Requirements – IEC 62267

- International committee worked for 8 years to create 62267
- Defined by Metro Systems with:
  - Driverless Train Operations (DTO)
  - Unmanned Train Operations (UTO)
- Automated Metro systems are now the norm in Europe and Asia for regional scale transit applications
- Other IEC standards describe the functional requirements of the Command and Control System
Levels of Automation in Transit

IEC safety standards for Automated Urban Guideway Transport (AUGT) systems addressed the UTO level of automation

- **STO** – Semi-Automated Train Operations
- **DTO** – Driverless Train Operations
- **UTO** – Unmanned Train Operations

Current discussion of Automated Vehicles would benefit from formally defining distinctions such as STO, DTO and UTO
Paris Metro –  
First Application of IEC Safety Standard

- Process started to convert old lines to unmanned fully automated operation

- Line 1 conversion has occurred while in service
  - 750,000 riders a day
  - Retrofit of full ATC
  - Platform edge doors

Grand Paris Express is a planned network of new lines that will ring Paris – all 200 kilometers will be fully automated.
IEC APPROACH TO THE GENERIC HAZARD ANALYSIS OF AUTOMATED TRANSIT SYSTEMS

Overview of Process Used by the IEC Working Group Responsible for Preparing Safety Requirements for Automated Urban Guided Transport
Generic Hazard Assessment Performed as an Element of IEC Standard Process

- Task Force Formed Under WG 39 and 45 to Develop an International Consensus on:
  - Hazards of Fully Automated DTO and UTO Operations
  - Appropriate Functional Safeguards to Mitigate Hazards

- Series of Meetings Built Progressive Consensus:
  - Format and Terminology
  - Hazard Identification and Categorization
  - Generic Safeguards to Mitigate Hazards


- Full Risk Analysis Still Required for Each Project
IEC Technical Report 62267-2
Hazard Analysis at Top System Level

• International Task Force worked for 5 years to create this Technical Report

• Companion Document to AUGT Safety Requirements IEC 62267

• Representation on Task Force: Large Metros, Equipment Suppliers, and Consultants

• Purpose: Understanding of Safety Issues Under Full Automation (Unmanned Train Operations)
<table>
<thead>
<tr>
<th>Case N°</th>
<th>Hazard</th>
<th>Cause</th>
<th>Trigger</th>
<th>Accident (Effect)</th>
<th>Safeguard</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Obstacle from outside the system</td>
<td>Guideways in tunnel: elements from outside protrude into the clearance of guideway e.g. drill</td>
<td>Train is approaching</td>
<td>Collision with obstacle, person might be injured e.g. derailment, collision, destroying of the carbody</td>
<td>1</td>
<td>External rules</td>
</tr>
<tr>
<td>1.1</td>
<td>Obstacle from outside the system</td>
<td>Guideways above ground: element from outside the system has fallen on the track e.g. tree, crane, car (vandalism included)</td>
<td>Train is approaching</td>
<td>Collision with obstacle, person might be injured e.g. derailment, collision, destroying of the carbody</td>
<td>2</td>
<td>Rules for checking guideway clearance</td>
</tr>
<tr>
<td>2</td>
<td>Physical barriers on bridges</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Physical barriers along the track</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Wayside obstacle detection device</td>
<td>Yes</td>
<td>Yes</td>
<td>Apply emergency brake to the trains entering into the area where an obstacle is detected</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Onboard obstacle detection device</td>
<td>Yes</td>
<td>Yes</td>
<td>Apply emergency brake. Combination with rules necessary</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>Onboard obstacle detection device</td>
<td>Yes</td>
<td>Yes</td>
<td>Applied emergency brake. Combination with rules necessary</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Hazard / Cause / Trigger / Accident (Effect)**

**Safeguard / Action Compensated for By Driver Intervention? / Action Satisfactorily Compensated for W/O Driver?**
### Published Report – Hazard Analysis Table

**Hazard / Cause / Trigger / Accident (Effect)**

<table>
<thead>
<tr>
<th>Case</th>
<th>Hazard</th>
<th>Cause</th>
<th>Trigger</th>
<th>Accident (effect)</th>
<th>No.</th>
<th>Safeguard</th>
<th>Remark</th>
<th>IEC 62267:2009</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.4</td>
<td>Obstacle in guideway clearance</td>
<td>Element from inside the system falling in the guideway clearance during operations (e.g. parts of a train, or the structure or wayside equipment)</td>
<td>Train is approaching</td>
<td>Collision with obstacle, person might be injured e.g. derailment, collision, destroying of the car body</td>
<td>1</td>
<td>Rules for checking guideway clearance</td>
<td></td>
<td>8.3.1</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>2</td>
<td>On board obstacle detection device</td>
<td>C</td>
<td>8.5.5</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>3</td>
<td>Design rules for trains</td>
<td>Out of scope</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>4</td>
<td>Design rules for structures</td>
<td>Out of scope</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>5</td>
<td>Design rules for wayside equipment</td>
<td>Out of scope</td>
<td></td>
</tr>
<tr>
<td>1.5</td>
<td>Obstacle in guideway clearance</td>
<td>Obstacle intrudes the guideway clearance at closed level crossing</td>
<td>Train is approaching</td>
<td>Collision with obstacle, person might be injured e.g. derailment, collision, damage to the car body</td>
<td>1</td>
<td>Level crossing supervision</td>
<td></td>
<td>8.7.12.2</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>2</td>
<td>Level crossing barrier</td>
<td></td>
<td>8.7.12.1</td>
</tr>
</tbody>
</table>

**Safeguard / Remark / IEC 62267 Ref. Section Number**

**NOTE:** Hazards common with those of manually driven/attended trains were not addressed in the generic HA – i.e., considered “Out of Scope”
# Structure of Hazard Analysis Table

## Hazards Associated with:

- **Ensuring safe movement of trains**
  - Safe route
  - Safe separation of trains
  - Safe speed
  - Safe accelerations/braking

- **Supervising guideway / preventing collisions with obstacles**

- **Supervising guideway / preventing collisions with persons**

- **Supervising passenger transfer (at stations)**
  - Door operations
  - Person between cars or between car and platform
  - Safe starting conditions

- **Operating a Train**
  - Putting into service or taking out of service
  - Supervising the status of a train under UTO

- **Detection and Management of Emergency Situations**