Modeling Risk for Positive Train Control (PTC) Systems

Craig W. Shier
craig.shier@lmco.com

Lockheed Martin
Risk Modeling on IDOT PTC

- The IDOT Positive Train Control (PTC) System prevents
  - Train-to-train collisions,
  - Derailments due to overspeed, and
  - Collisions between trains and roadway workers or their equipment while working within their authority limits

- Safety Requirements for PTC
  - Draft Rule CFR §236 subpart H
  - Base case definition

- Risk Model
  - Input
  - Design of the Risk Model
  - Model Validation
  - Output

- Future of the Risk Model
IDOT PTC System Architecture
Safety Requirements for Positive Train Control

- **CFR Title 49 Parts 209, 234, and 236**
  - Standards for Development and Use of Processor-Based Signal and Train Control Systems; Proposed Rule

- **§ 236.909 Minimum Performance Standard**
  - Establish with a high degree of confidence that introduction of the product will not result in risk that exceeds the (adjusted) previous condition.

Relative Risk Assessment

Risk (New) ≤ Risk (Old)
Safety Requirements for Positive Train Control

- Risk Analysis Process

  - Risk levels must be adjusted for Exposure expressed as total train miles or total passenger miles traveled per year.

  - Severity must identify the total cost, including fatalities, injuries, property damage, etc.

  - System View of train control system in addition to MTTHE view at the subsystem level

- “Previous condition” defined as 4 aspect in-cab signal with enforcement of unacknowledged downgrade in aspect (no speed enforcement)

  - Simulation is the most effective means of accounting for these factors.
## Input to Risk Model

<table>
<thead>
<tr>
<th>Input Elements</th>
<th>Challenges</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Railroad Parameters</strong></td>
<td></td>
</tr>
<tr>
<td>Track Configuration</td>
<td>Level of Detail</td>
</tr>
<tr>
<td>Local Environment</td>
<td>Statistical Variation</td>
</tr>
<tr>
<td>Train Characteristics</td>
<td>Applicability of Rules</td>
</tr>
<tr>
<td>Timetable or Schedule</td>
<td></td>
</tr>
<tr>
<td>Train Movement Priorities</td>
<td></td>
</tr>
<tr>
<td><strong>Human Factors</strong></td>
<td></td>
</tr>
<tr>
<td>Stimulus-Response Pattern</td>
<td>Quantification</td>
</tr>
<tr>
<td>Correlation of Actions</td>
<td>Sequences of Actions</td>
</tr>
<tr>
<td>Human-Human Interactions</td>
<td></td>
</tr>
<tr>
<td><strong>Train Control System</strong></td>
<td></td>
</tr>
<tr>
<td>Equipment Characteristics</td>
<td>Field Performance vs Mil Hndbk 217</td>
</tr>
<tr>
<td>System Characteristics</td>
<td>System Influence on Human Behavior</td>
</tr>
<tr>
<td>Human-System Interactions</td>
<td></td>
</tr>
<tr>
<td>System Maint Practices</td>
<td></td>
</tr>
<tr>
<td>Operating Rules &amp; Practices</td>
<td></td>
</tr>
</tbody>
</table>

**Model the Factors that Reveal Differences in Risk**
ASCAP Model (Axiomatic Safety-Critical Assessment Process)

Reliability Modeling & Measurements
- Equipment Configurations
- Failure Rates
- Maintainability Factors

Train Movement
- Train Dynamics
- Network Geometry
- Timetables
- Rulebook

Human Factors Assessment
- Agent Behavior (Correct, Erroneous, Non-Responsive)

Discrete Event Monte Carlo Simulation (Multi-rate)

Failure Generator
- RR Network Models
- Object Models

Events Of Interest
- Agent Models

Severity Assess
- Risk Metric

Validation Data

Assess

Assess

Assess

Assess
Object Model

Legend
- Monte Carlo selection
- $C_R$: Repair coverage (human error)
- $C_{int}$: Internal fault coverage

Diagram:
- Fail Unsafe State
- Operational State
- Fail Safe State
- Covered?

- $1 - C_R$: Repair
- $C_R$: Repair coverage (human error)
- $C_{int}$: Internal fault coverage
- 1 - $C_{int}$: Fault
- Repair
- Unnecessary repair
- Additional fault
- Transient recovery
Agent Model

Stimulus

Recognition

Compliance

Correct Action (Rulebook Compliant)

Non-Compliance

Erroreous Actions (Rulebook Non-Compliant)

Non-Responsive

Non-Recognition

P_{Recognition}

P_{Compliance}

P_{Non-Compliance}

P_{Non-Recognition}
Model Validation

- **Challenge: Calibration with historical data**
  - Severe accidents are very low probability (≈10E-8 / train mile)
  - Accident reporting process not precise enough for risk analysis of train control systems
  - “Close calls” are not recorded, i.e. exposure is unknown

- **Techniques**
  - Expert Reviews of Input and Assumptions
    - Expert panels representing Railroads, Labor, Suppliers, FRA
  - Component testing
    - Apply CMMI type software discipline to model testing
  - System Testing
    - Statistical summarization of output
  - Sensitivity analysis
    - Model range of uncertainty in critical input parameters
### Event Logs

**Incident/Accident Type:** Broken Rail Derailment (EOI 185)

**Train Info:** ID = LSF 50 (Freight), 27 cars, 2 locomotives

**Train Movement:** Northbound, 60 mph at rail intersection, Average Spd Model

**Incident/Accident Date:** Friday, Day 27116, Spring

**Incident/Accident Severity and LOO:** $166,017.00, LOO TBD

**Cab Signal Status:** Cut-Out (failed prior to entry into system)

**Wayside Signal System Status:** All OP except FUS Rail between 138.67–136.90

<table>
<thead>
<tr>
<th>#</th>
<th>Time</th>
<th>Mile Post</th>
<th>Event Type</th>
<th>Speed Limit</th>
<th>Actual Speed</th>
<th>Details</th>
<th>Direct Cause</th>
</tr>
</thead>
<tbody>
<tr>
<td>06</td>
<td>10:49:52 AM</td>
<td>139.17</td>
<td>Visual Look-Ahead: Control Point Signal (at 138.67)</td>
<td>60</td>
<td>60</td>
<td>Aspect=Green, Train Crew is Compliant and proceeds</td>
<td>Yes</td>
</tr>
<tr>
<td>05</td>
<td>10:50:08</td>
<td>138.90</td>
<td>Visual Look-Ahead: Intermediate Signal (at 136.9)</td>
<td>60</td>
<td>60</td>
<td>Aspect=Green, Train Crew is Compliant and proceeds</td>
<td></td>
</tr>
<tr>
<td>04</td>
<td>10:50:22</td>
<td>138.67</td>
<td>Intersection: Rail (for previous block)</td>
<td>60</td>
<td>60</td>
<td>Rail=Operational (OP)</td>
<td></td>
</tr>
<tr>
<td>03</td>
<td>10:50:22</td>
<td>138.67</td>
<td>Intersection: Control Point Signal (at 138.67)</td>
<td>60</td>
<td>60</td>
<td>Aspect=Green, Train Crew is Compliant and proceeds</td>
<td></td>
</tr>
<tr>
<td>02</td>
<td>10:50:22</td>
<td>138.67</td>
<td>Intersection: Switch</td>
<td>60</td>
<td>60</td>
<td>Switch=Operational (OP), normal position</td>
<td></td>
</tr>
<tr>
<td>01</td>
<td>10:51:38</td>
<td>137.40</td>
<td>Visual Look-Ahead: Intermediate Signal (at 136.9)</td>
<td>60</td>
<td>60</td>
<td>Aspect=Green, Train Crew is Compliant and proceeds</td>
<td></td>
</tr>
<tr>
<td>I/A</td>
<td>10:52:08</td>
<td>136.90</td>
<td>Intersection: Rail (for previous block)</td>
<td>60</td>
<td>60</td>
<td>Rail=Failed–Unsafe (FUS), not detected by track circuit, results in Broken Rail Derailment Incident/Accident</td>
<td></td>
</tr>
</tbody>
</table>
Preliminary Base Case
ASCAP Likelihood Results

Mishaps versus Train Miles

No. of Mishaps

Train Miles Accumulated

- Cab Signaling
- Partially Fitted Cab Signaling
- SS Interlocking Only
- Relay Interlocking Only
Future of Sim-Based Risk Assessment

Configurable Parameters And Rules
RR and Suppliers

Railroad Parameter Files
- Track Configuration
- Local Environment
- Train Characteristics
- Timetable or Schedule
- Train Movement Priorities
- Operating Rules & Practices

Hum Fact Parameter Files
- Stimulus-Response Pattern
- Correlation of Actions
- Human-Human Interactions

Train Ctrl Parameter Files
- Equipment Characteristics
- System Characteristics
- Human-System Interactions
- System Maint Practices

Simulation Driver
Simulation Specialist

Simulation Control Software
Core Engine

Incident, Accident Logs and Statistics

FRA Oversight, AAR Consultation
Accomplishments

• **Established a System Level risk assessment process that supports the new regulatory requirements for Train Control Systems**

• **Developed a Train Control Simulation**
  - Incorporates Human, System and Operational hazards
  - Models exposure to safety hazards
  - Methods for handling uncertain inputs

• **Established a team of experts**
  - Suppliers provide product safety data
  - Railroads provide operational data
  - Various experts provide assessment and validation