Modeling Risk for Positive Train Control (PTC) Systems

Craig W. Shier

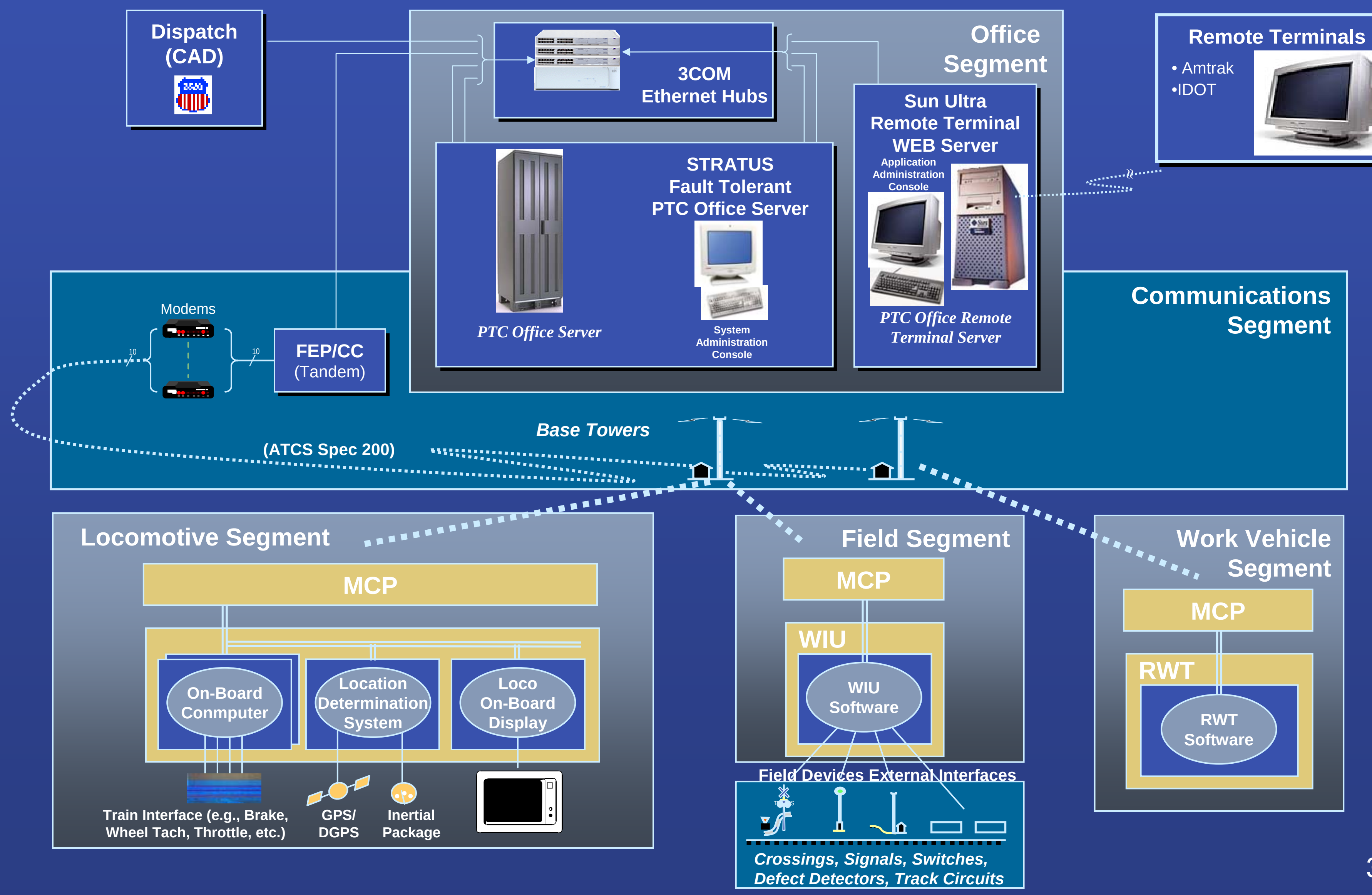
craig.shier@lmco.com

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 <u>risk</u> 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)***

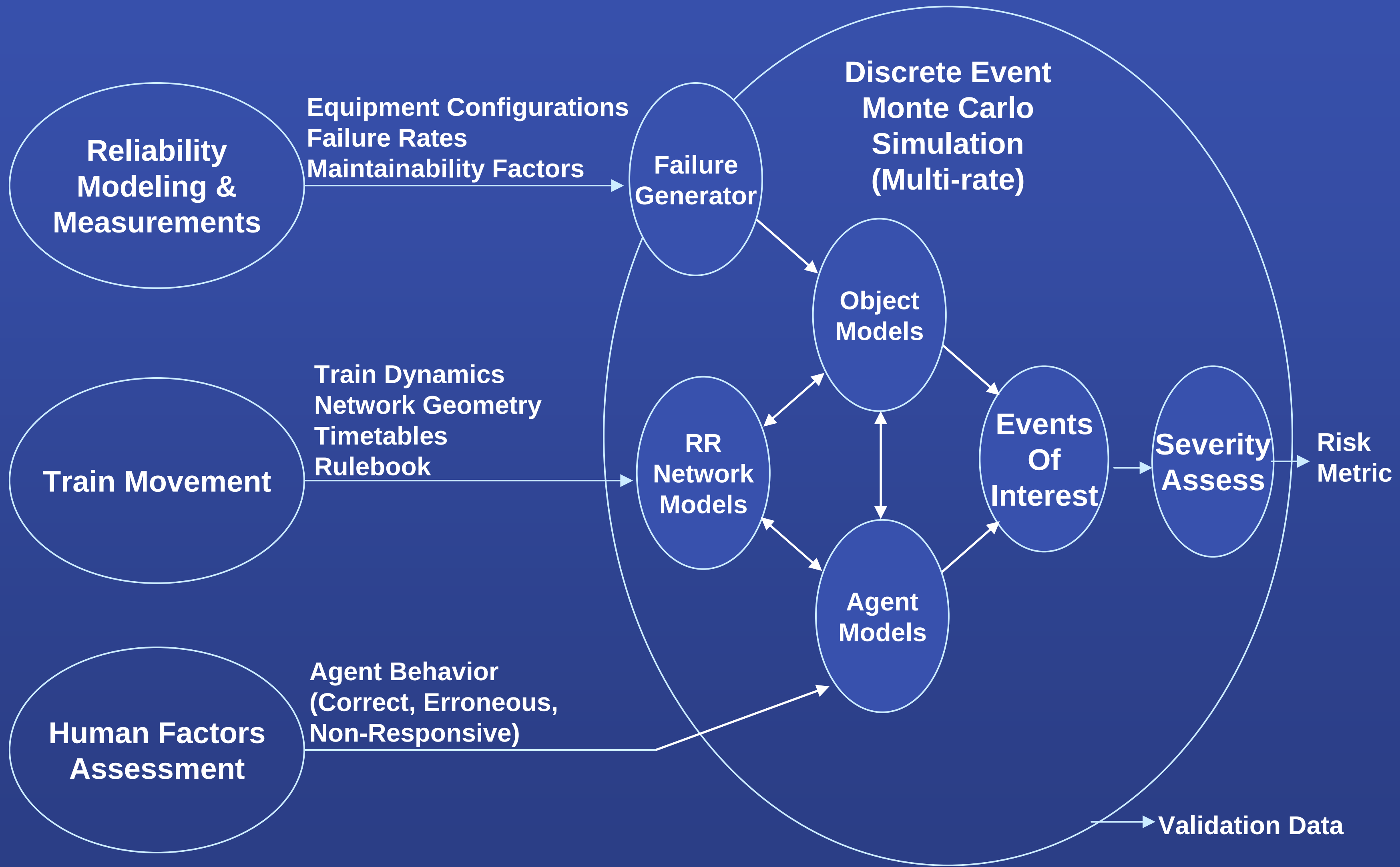
> ***❖ Simulation is the most effective means of accounting for these factors.***

Input to Risk Model

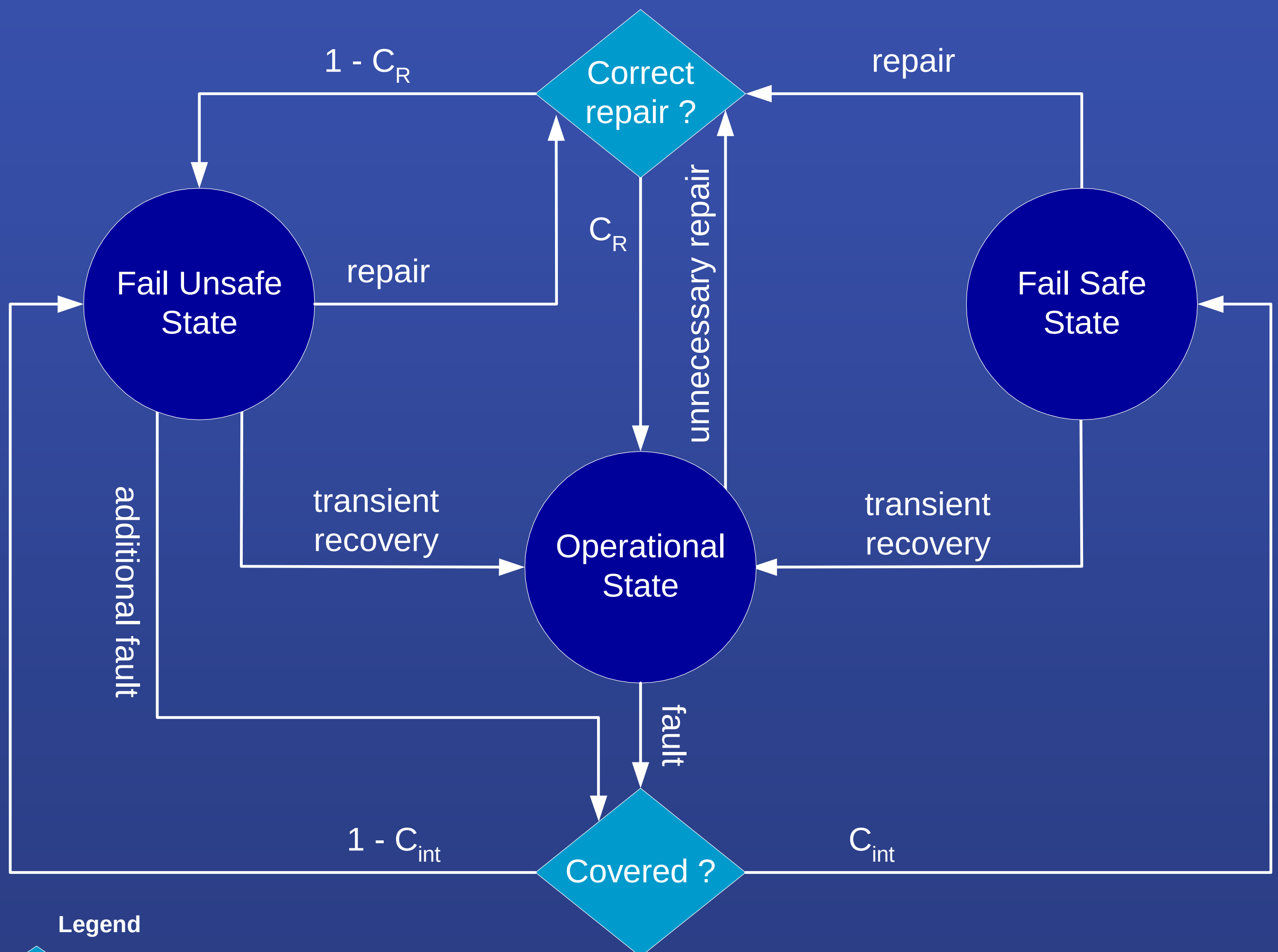
	Input Elements	*Challenges*
Railroad Parameters	Track Configuration Local Environment Train Characteristics Timetable or Schedule Train Movement Priorities	Level of Detail Statistical Variation Applicability of Rules
Human Factors	Stimulus-Response Pattern Correlation of Actions Human-Human Interactions	Quantification Sequences of Actions
Train Control System	Equipment Characteristics System Characteristics Human-System Interactions System Maint Practices Operating Rules & Practices	Field Performance vs Mil Hndbk 217 System Influence on Human Behavior

Model the Factors that Reveal Differences in Risk

ASCAP Model (Axiomatic Safety-Critical Assessment Process)



Object Model

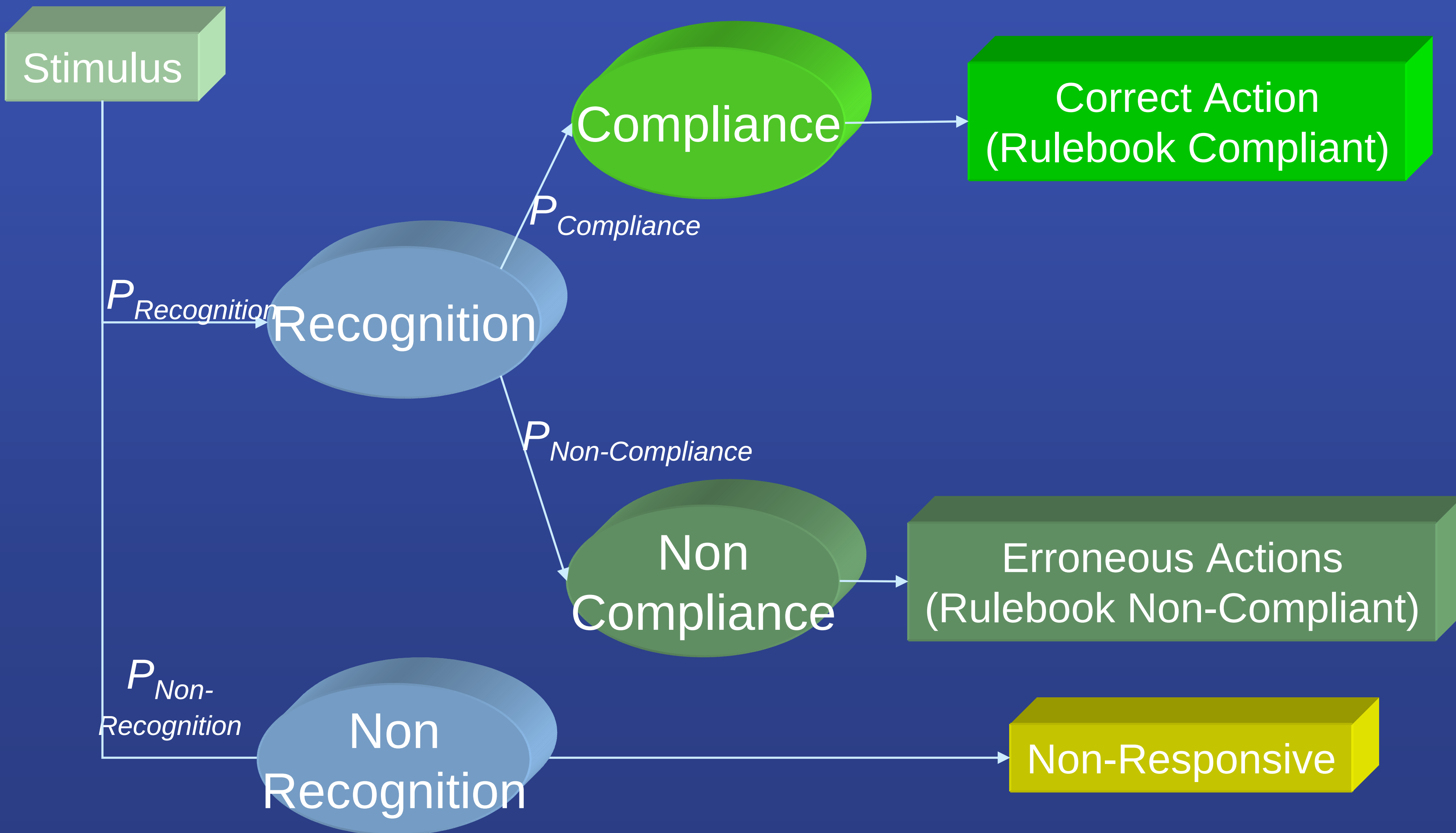


Legend

◆ Monte Carlo selection

C_R : Repair coverage (human error)
C_{int} : Internal fault coverage

Agent Model


Stimulus
P Recognition
Recognition
P Compliance
Compliance
Correct Action
(Rulebook Compliant)
P Non-Compliance
Non Compliance
Erroneous Actions
(Rulebook Non-Compliant)
P Non-Recognition
Non Recognition
Non-Responsive

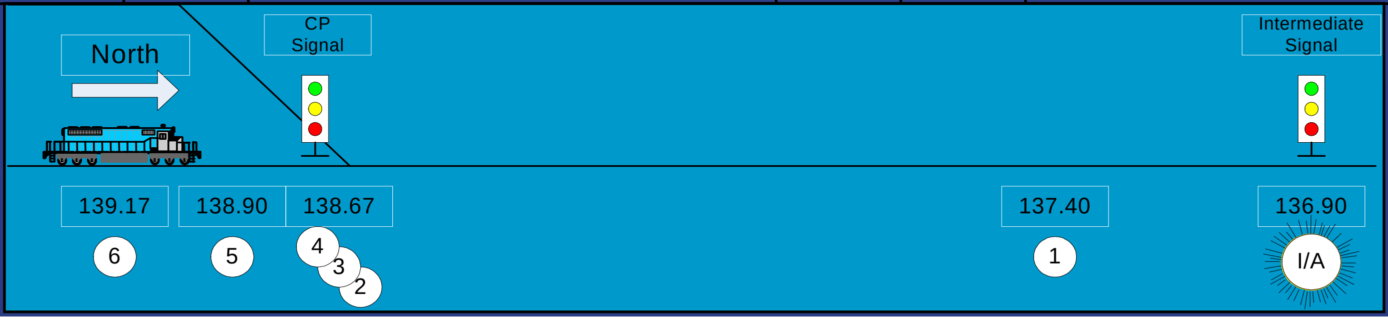
Model Validation

- ***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	Cab Signal Status: Cut-Out (failed prior to entry into system)
Incident/Accident Severity and LOO: $166,017.00, LOO TBD	Wayside Signal System Status: All OP except FUS Rail between 138.67-136.90

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



Preliminary Base Case
ASCAP Likelihood Results

Future of Sim-Based Risk Assessment

Configurable Parameters And Rules
RR and Suppliers

Simulation Driver
Simulation Specialist

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 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**