Illinois Department of Transportation Positive Train Control (IDOT PTC) Project

IDOT PTC Safety Program

Warren Klinck

December 4, 2001

Topics

- System Safety Program
- Safety Assurance Process / Concepts
- Safety Critical Functions
- Design Documentation
- Hazard & Risk Analyses
- Hazard Coverage Handling
- Validation & Verification
- Requirements
- ASCAP and Base Case
- Program Evolution With RSAC
- Approval

System Safety Program

- **System Spec V3.1 objectives**
  - Use COTS hardware and software
  - “Total system safety approach, rather than relying only on fail-safety of individual system components” (4.11.1.c)
  - “Closed Loop safety design” (4.11.1.g)
  - Handle authority issuance and enforcements in a Vital manner (4.2.1)
  - Safety analyses based upon the emerging Processor Based Rule (NPRM)

System Safety Program

- **Safety Requirements Sources**
  - System Spec Version 3.1
  - System SOW Version 3.0
  - NPRM RSAC Draft Rule (approval pending)
  - Railroad Safety Program Plan (RSPP)(to be released shortly)

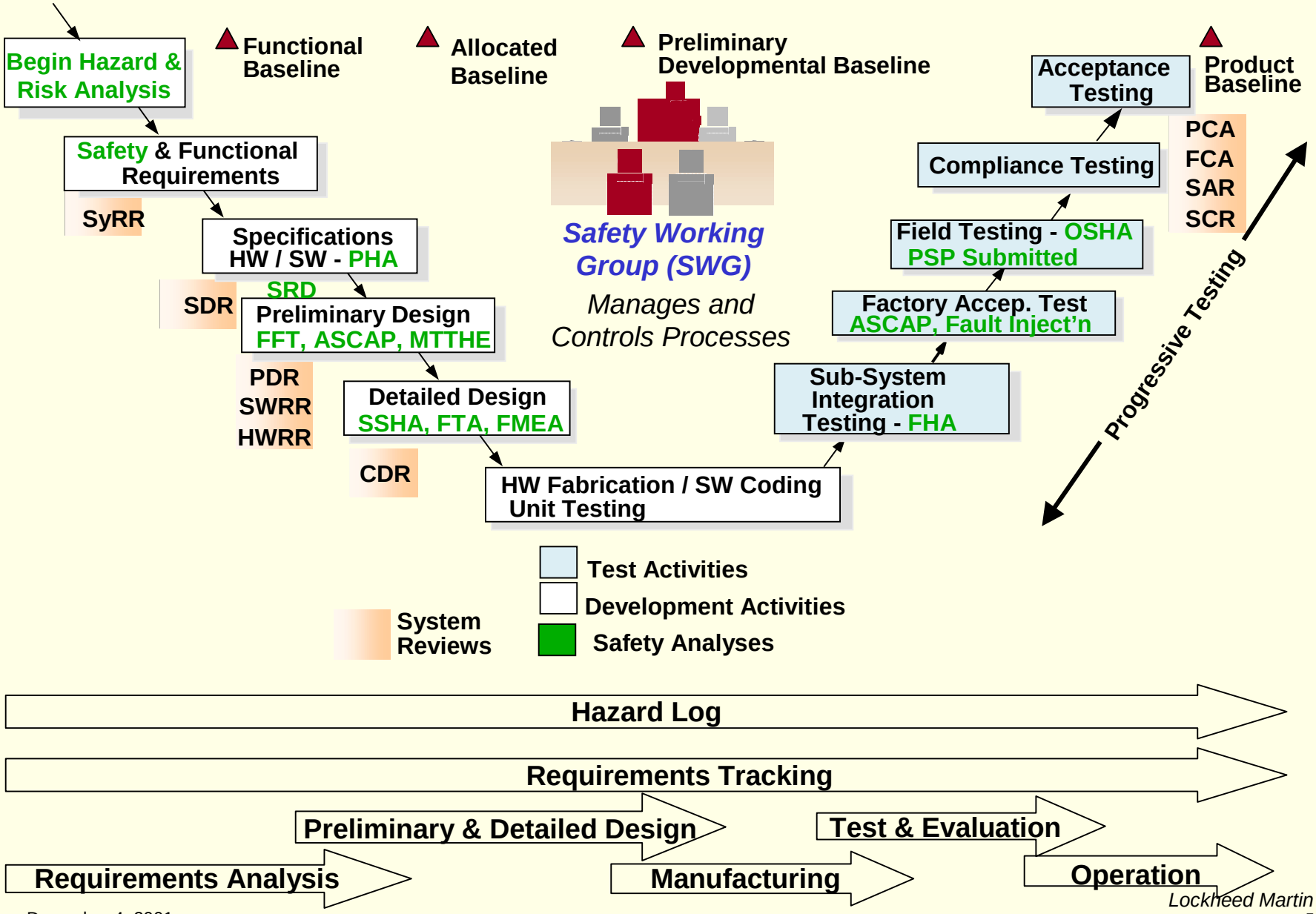
Safety Assurance Process

- **Safety Program parallels the system development effort (Figure 1)**
- **Safety analyses are scheduled to support design effort**
  - Key hazard analyses and UVA simulations coincide with major design reviews
  - Derived requirements from hazard analyses will be added to Hardware Requirements Specification (HRS), Software Requirements Specification (SRS) and requirements tracking database
- **Derived requirements from Safety analyses incorporated into requirements tracking database**
  - Safety critical requirements tracked from early design through verification

Safety Assurance Process

- **Derived requirements from Safety analyses incorporated into Requisite Pro database**
  - Safety critical requirements tracked from early design through testing
- **Contract Data Requirement List items (CDRL's) developed during course of the program (see Formal Documentation) form part of the PSP**
- **Safety is designed in on a system level**
  - Closed loop design principles (e.g. request, grant, acknowledge)
- **Incremental release of PSP contents is being forwarded to TTCI by LM throughout the program**
  - CDRL's & Safety Analyses to the Program Office / System Engineer (SE)

Figure 1 - Safety Critical System Development



Safety Assurance Concepts

- **Hardware safety assurance concepts overview (Reference IEEE 1483-2000)**

Segment	Approach
Office Server	Checked Redundancy
Locomotive	Checked Redundancy, Segment to Segment cross checking
Field	Diversity and self-checking
Work Vehicle (includes Roadway Worker Terminal)	Segment to segment cross checking; Closed Loop Confirmation and acknowledgement of all transmitted data
Communications Segment	ATCS 200 system transmits vital messages with Cyclic Redundancy Checks (CRC's)

Safety Critical Functions

- **IDOT PTC Safety Critical Functions include**
  - PTC Authorities
  - Enforcements (authority or speed violation)
  - Advanced crossing activation
  - Train location determination
  - Authority display to Roadway Workers
  - Manage track data base (including speed limits)
  - Broadcast Warnings / Emergency Response
  - Power switch control
  - Moving block / Safe braking

Safety Critical Functions (cont)

- **IDOT PTC Safety Critical Functions (cont)**
  - Monitoring route integrity
  - Safety of local signal control (equal to CTC functions)
  - Train integrity
- **Safety Allocations documented in Safety Requirements Document (SRD), Part 4 of the Product Safety Plan (PSP)**
  - Allocates all functions as either safety critical (or not)

Design Documentation

- **Design documentation forms part of the PSP**
  - System Level
    - System Segment Design Doc (SSDD) (CDRL C010)
    - Requirements Allocation Matrix (RAM) (CDRL C009)
    - Contractor Master Test Plan (CMTP) (CDRL C010)
  - Hardware
    - HW Development & Integ'n Plan (HDIP) (CDRL C003)
    - HW Requirements Specification (HRS) (CDRL C008)
    - Hardware Design Document (HDD) (CDRL C013)
  - Software
    - Software Development Plan (SDP) (CDRL C002)
    - Software Requirements Spec (SRS) (CDRL C007)
    - Software Design Document (SWDD) (CDRL C012)
  - Interface
    - Interface Requirements Specification (IRS) (CDRL C006) / Interface Design Document (IDD) (CDRL C011)

Hazard And Risk Analyses

- **Hazard analyses to be performed: PHA, SRD, FFT, SSHA, FTA, FMEA, FHA and O&SHA**
- **Recent Activity**
  - PSP Containing Document generated (see Figure 2)
    - Defines 20 sections of PSP
    - Complies with NPRM and RSPP
    - Uses CDRL's generated as a part of system design effort
    - Defines data to be submitted at major submission in June 2002
    - Defines interaction of ASCAP and conventional hazard analyses

Figure 2- Product Safety Plan (PSP)

Hazard And Risk Analyses (cont'd)

- **Recent Activity (Cont)**
  - Preliminary Hazard Analysis (PHA) submissions on 9 April, June 15, 22 October and 29 October
    - PHL in RSPP completely revised to reflect more complete list of hazards
    - Safety Focus Group has reached agreement on hazard effects, risk indexes and mitigations
    - Content and traceable numbering of mitigations resolved
    - Final version being revised per comments of broader Safety Working Group

Hazard And Risk Analyses (cont'd)

- Safety Requirements Document (SRD) generated
  - Contains the "Safety Matrix"
    - SS V3.1 SSR's annotated as "safety critical" functions (or not)
    - Designation reside in the master requirements data base
  - Vehicle for entering data into requirements tracking data base
  - Safety-Critical / Non- Safety-Critical rating based on safety guidelines furnished with matrix
  - SRD and guidelines were developed with inputs from SE

Hazard And Risk Analyses (cont'd)

- Functional Fault Tree (FFT) submitted
  - Top level tree under review by SE
  - Iteration and development being handled by Safety Working Group
  - Rapid completion targeted to support CDR

Hazard Coverage Handling

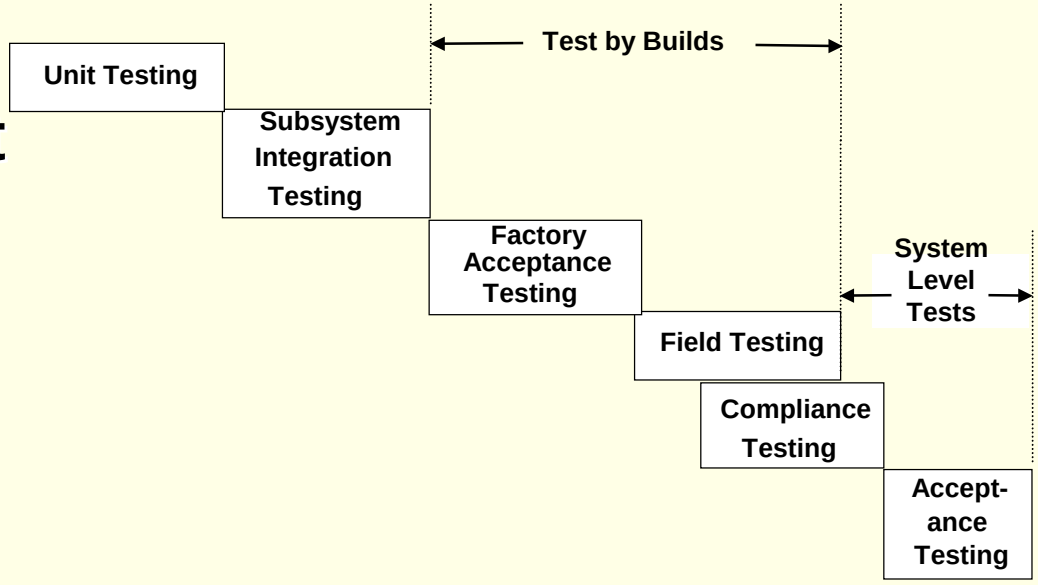
- **Modeling performed by UVA to assess segment Mean Time to Hazardous Event (MTTHE)**
  - Coverage model is defined using λ ‘s and coverage values for sub-elements of each segment
  - Calculated MTTHE’s compared to values used in ASCAP simulations
- **Coverage values for each segment proved out by fault injection tests performed by UVA**
  - Coverage values derived from testing compared with those used in MTTHE models

Validation and Verification

- **Validation**
  - **A structured and managed set of activities which demonstrate that the system, as specified and implemented, performs the intended functions and that those functions result in overall safe operation. *Validation* answers the question, "Did we build the *right system*? (Ref: IEEE 1483-2000)**
- **Verification**
  - **A structured and managed set of activities which identify the vital functions required to be performed by the system, and demonstrate that the system, including its subsystems, interfaces and components, implements the vital functions fail-safely to a level that meets the allocated system safety goals. *Verification* answers the question, "Did we build the *system right*?" (Ref: IEEE 1483-2000)**
- **Progressive Testing used to accomplish Validation**
  - Ensures system performs intended functions

Validation and Verification (Cont)

- **Requirements tracking performed using Requisite Pro**
  - Provides requirements traceability through all design and test documentation
- **Documented via the RAM and each technical CDRL**
- **Used as a basis for "bottom up" system testing**
- **Phases of Systems Test**



Validation and Verification (Cont)

- **Field Testing, Compliance Testing, Acceptance Testing, FTA and FMEA's verify that the overall system operates safely in its intended environment**
- **At the conclusion of Progressive Testing**
  - Perform audit on Configuration
  - Revenue Service after acceptance by RR and FRA
- **Important test related CDRL's delivered to date:**
  - Contractor Master Test Plan (CMTP) CDRL D001
  - Software Development Plan (SDP) - CDRL C002
  - Hardware Development & Integration Plan (SDP) - CDRL C003

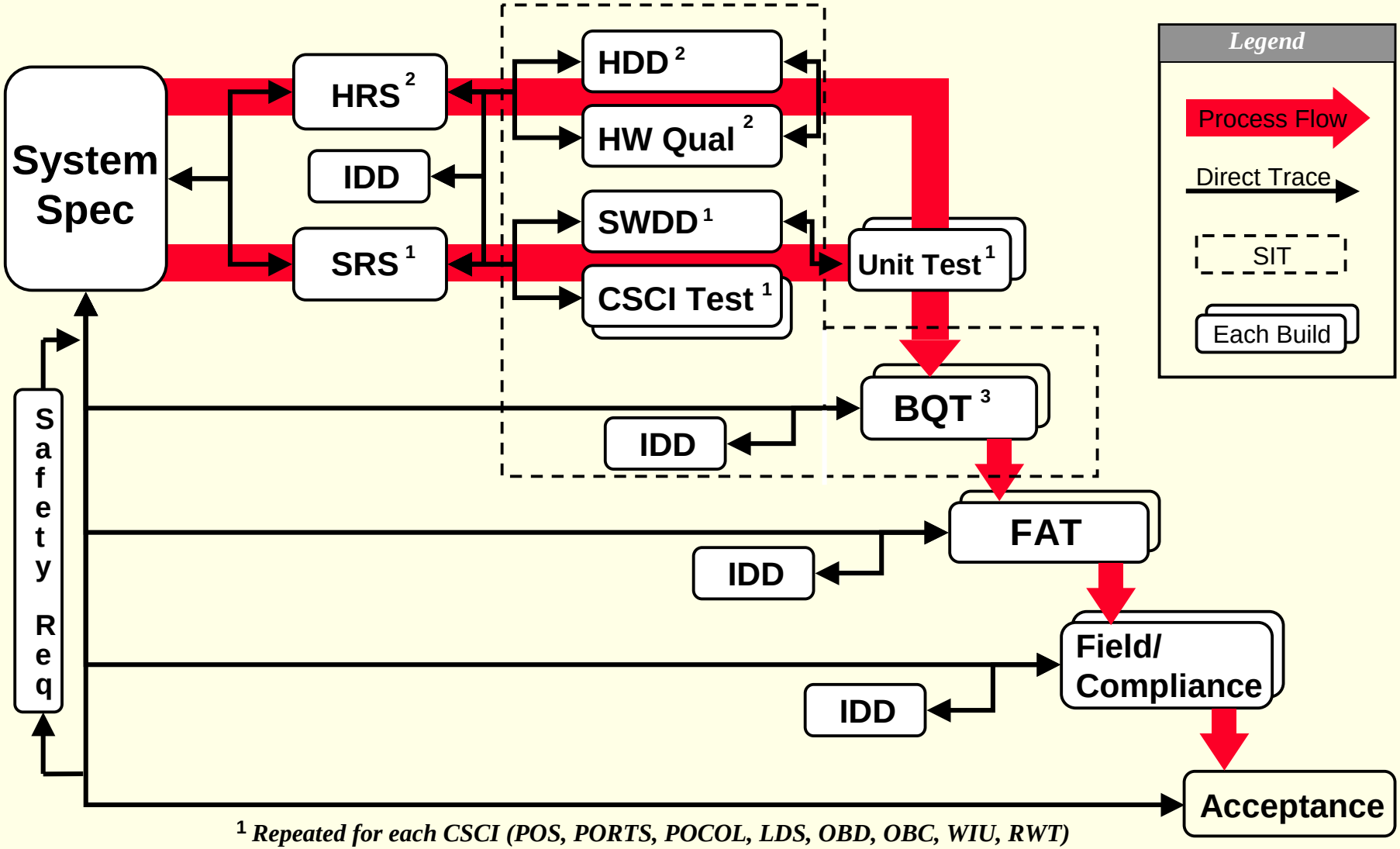
Validation and Verification (Cont)

- **LM verification approaches include:**
  - ASCAP simulations by UVA to define numeric safety values (accidents / million train miles)
    - Accident / hazard occurrence predicted to be in same proportion before and after PTC
  - MTTHE modeling by UVA to assess compliance with ASCAP segment safety budgets
  - Fault injection testing by UVA to confirm coverage values and MTTHE used in modeling

Requirements

- **System Spec is source of 678 SSR's**
- **Requirements traceability done using Requisite Pro tool**
  - SRD has been generated from Req Pro
- **Hazard Log uses separate data base for safety**
  - Hazards are tracked to closure for
    - Design mitigations
    - Verification of mitigations
  - Test procedures / reports that test for a safety critical SSR will form a part of the PSP
- **Derived requirements flow from safety analyses and requirements specifications (HRS, SRS, IRS) (See Figure Next Page)**

Requirements/Test Trace Overview

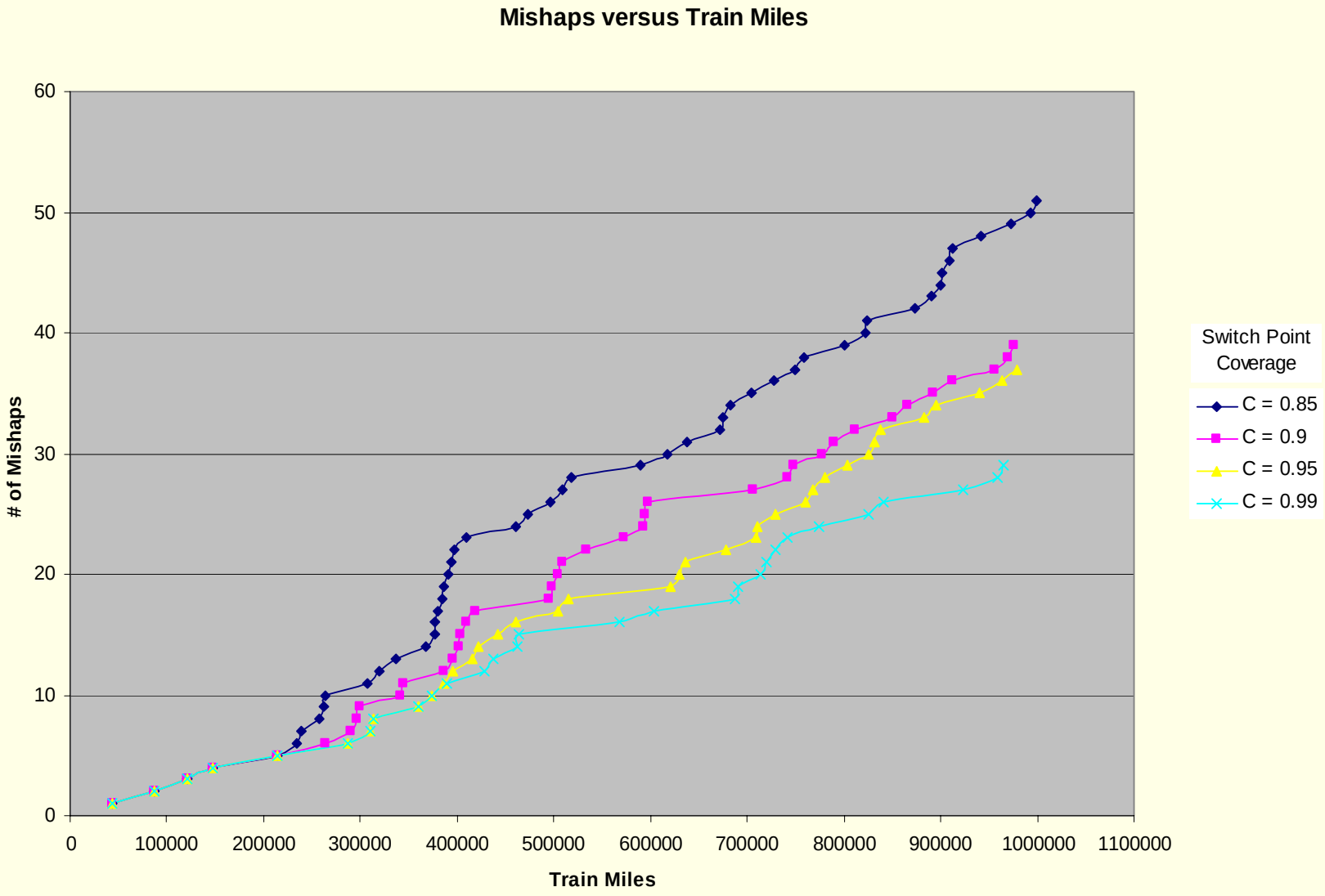


[1] *Repeated for each CSCI (POS, PORTS, POCOL, LDS, OBD, OBC, WIU, RWT)*
[2] *Repeated for each HWCI (POS, PORTS, LDS, OBD/OBC, WIU, RWT)*
[3] *Repeated for each Segment (Office, Loco, Field, Work Vehicle)*

ASCAP and Base Case

- **ASCAP simulations**
  - Models hardware, software, operating rules, human interaction
  - Simulates events sequences leading to hazard
  - Models failure probabilities and random failures
  - Verifies system design (no faults)
  - Injects faults into system with Monte Carlo (random number) stimulation of failures
    - Verifies fail safe response
- **Five (5) ASCAP simulations are currently tasked**
  - Base Case is first simulation (uses 4 aspect cab signal)
  - Progressive simulations will model modular subsets of functions, culminating in full system functionality

Typical UVA ASCAP Output Plot



ASCAP and Base Case (continued)

- **UVA Safety Case documents are generated to organize & present ASCAP data**
  - ASCAP runs produce data files that are reduced to
    - Develop plots of accidents per million train miles
    - Describe event sequences leading to an accident
    - Describe input data and assumptions
- **Mean Time To Hazardous Event (MTTHE) prediction is used as input to ASCAP**
  - Analyzes each IDOT PTC segment relative to “budgets” established from ASCAP
  - Follow on fault injection tests by UVA confirm MTTHE budgets are met

ASCAP and Base Case (continued)

- **Base Case uses the following:**
  - Assumes 110 MPH hypothetical operation with Cab Signal system per FRA direction
    - Territory is currently 79 MPH with no Cab Signaling
  - Data provided for Base Case
    - RR schedules, Train Consists, Locomotives types
    - Dispatch algorithm
    - Traffic density (current, projected and worst case future)
    - Territory data defining all “objects” (control points, switches, highway crossings, RR crossings, etc.)
    - Precision Measurement Vehicle (PMV) track data
    - Route & aspect drawings
    - Braking algorithm
    - UPRR Rule Book
    - Sample of actual Bulletin data

Program Evolution With RSAC

- **LM's PSP meets the requirements of the emerging Processor Based Rule (NPRM)**
  - ASCAP simulations provide numerical measure of safety
    - PTC will be assessed against a Base Case system defined IAW NPRM guidelines
    - Output of ASCAP is predictions of accidents per million train miles
    - IDOT PTC must show safety equal or greater than Base Case (lower risk)
  - Conventional hazard analyses also performed to provide assurance that system functions adequately mitigate potential hazards
  - MTTHE for each segment assessed as called for in NPRM

Approval Process

- **Formal PSP is submitted to FRA by UPRR / AMTRAK**
  - LM generated PSP provides input and detailed analyses
  - Initial PSP submission date is June 2002
- **Compliance Testing and Acceptance Testing will be performed after this initial submittal**
  - A PSP Addendum will be submitted in December 2002 providing safety related test reports from Compliance Testing and Acceptance Testing
  - Incremental delivery of PSP contents are forwarded to TTCI by LM throughout the program
    - CDRL's & Safety Analyses to the System Engineer (SE)