Implementation of a Stochastic Timeline Validation Tool Integrated with R2U2

James B. Dabney, University of Houston – Clear Lake
Michael Whitzer, NASA JSC
Pavan Rajagopal, Snigdha Palamari, Sonali Thakkar, CACI
Chris Pohlen, Hemanth Koralla, Amentum
Andrew Albright, METECS

March 2026

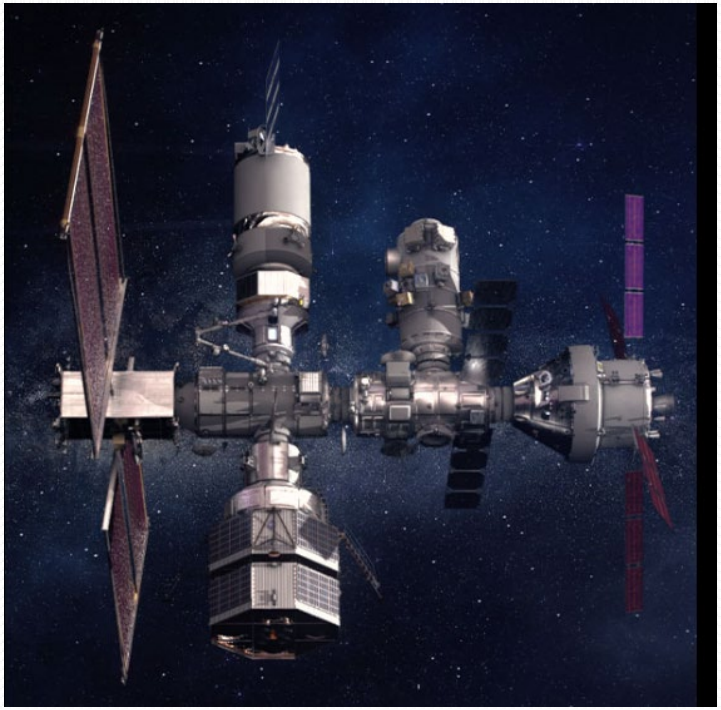
This publication does not contain information which falls under the purview of the US Munitions List (USML), as defined in the International Traffic in Arms (ITAR), 22 CFR 120-130, and is not export controlled. This publication does not contain information within the purview of the Export Administration Regulation (EAR), 15 CFR 730-744, and is not export controlled. This document (DAA 20240004187) has been reviewed in STRIVES.

Overview

- Background
  - Gateway VSM Autonomy
  - Timeline definition
  - Mission databases
- Timeline modeling
- Incorporating efficient probability density functions
- Generating Monte Carlo trials and traceability metadata
- Automatic generation of assume-guarantee contracts
- Integration with R2U2 and mapping failures to timeline tasks
- Lessons learned and future work

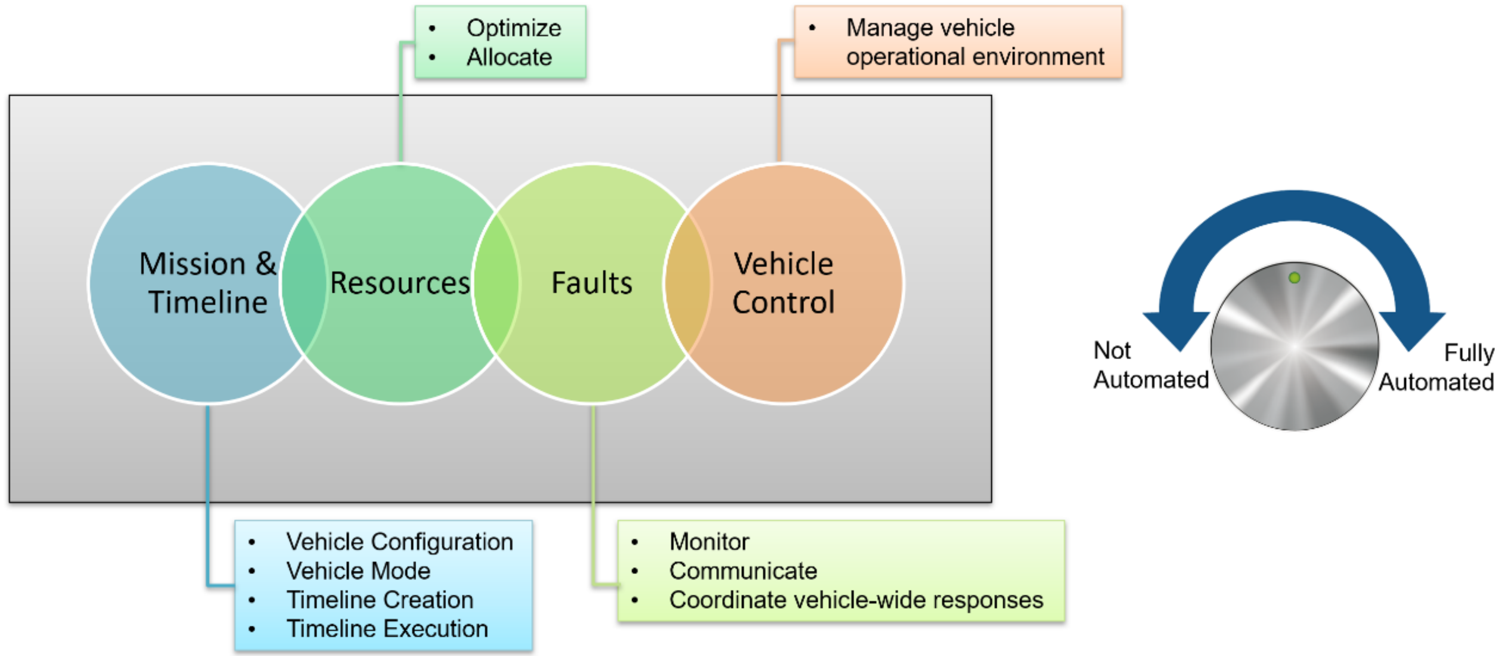
Lunar Gateway

- Artemis space station in cislunar (NRHO) orbit
- Gradual buildup of modules
- Initial Co-Manifested Vehicle
  - Habitation and Logistics Outpost (HALO)
  - Power and Propulsion Element (PPE)
- Sustaining
  - International Habitation Module (IHAB)
  - Airlock
  - Visiting vehicles – Orion spacecraft



Vehicle System Manager

- Four management functions
- Coordinates module functions at vehicle level; interfaces with humans and visiting vehicles
- Fully autonomous when uncrewed and no active ground control
- Can dial down autonomy to permit concurrent vehicle control by flight crews and ground



Timeline Definition

- Sequence of tasks to accomplish mission objectives
- Can run for extended time periods
- Simple task single action at specified time and specified duration
- Compound tasks (TrEX) that contain branching, event triggers, handle uncertainty
- A timeline can be a complex state machine with many branches and parallel activities

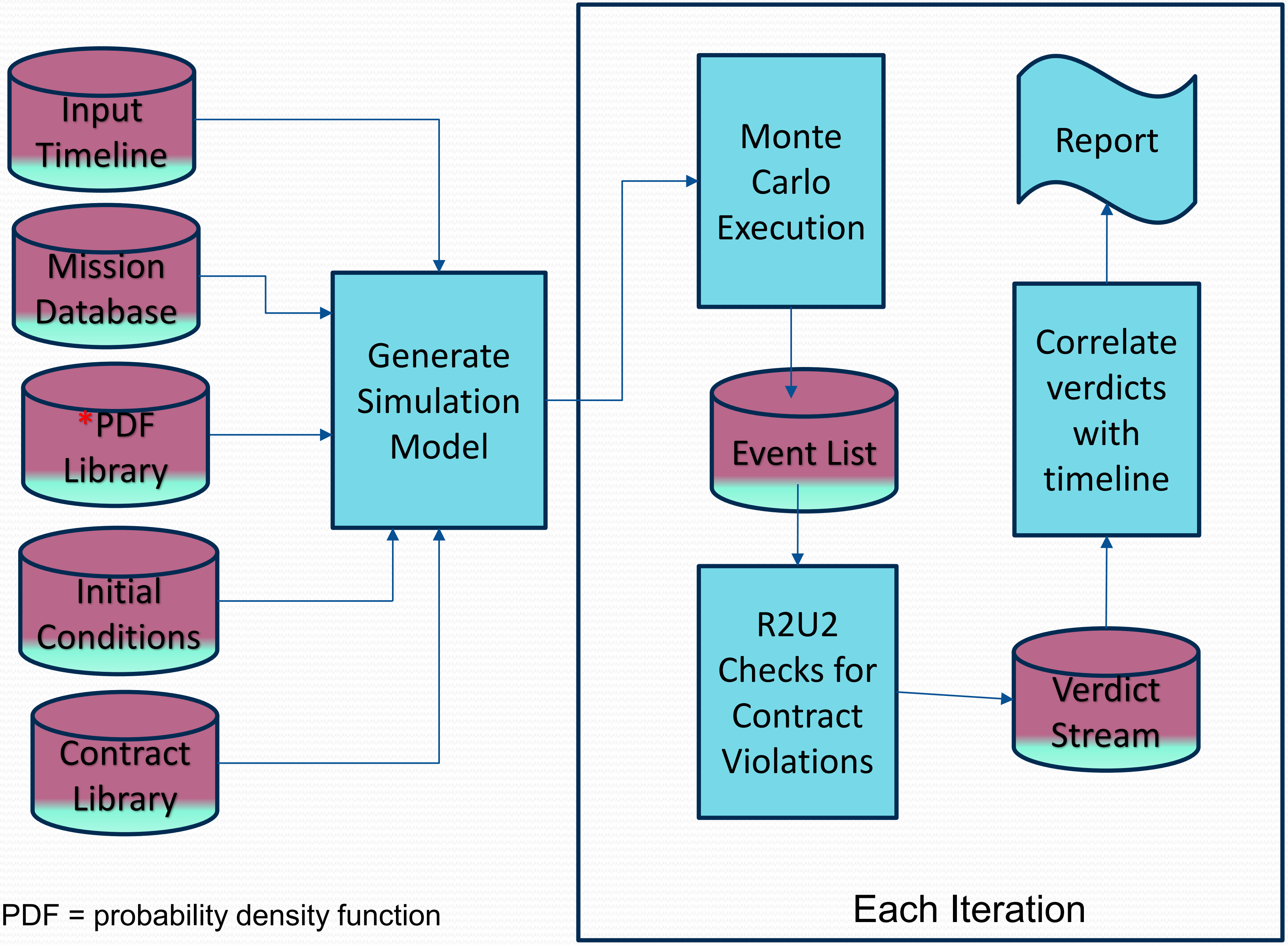
Gateway VSM Timelines

- Created and validated on the ground
- Uplinked to Gateway
- Executed autonomously or semi-autonomously (when crewed)

Timeline Validation Alternatives

- Model checking (such as TLA+/PlusCal)
  - Complete coverage of state-space
  - Requires tool to convert timeline into state machine model
  - Susceptible to state-space explosion due to complexity of timelines
- Direct simulation
  - Monte Carlo simulation using flight software test facility
  - Excellent fidelity
  - Test system runs at real time or small multiple of real time
- Discrete event timeline simulation
  - Potential for rapid execution as each step is an event
  - Requires models of tasks and TrEX procedures
- Selected approach
  - Discrete event timeline simulation
  - Augmented with small number of direct simulation cases

Stochastic Validation Flow



*PDF = probability density function

Mission Databases and Inputs

- Mission databases contain a variety of data needed to operate VSM
    - Task definitions
    - Constraints
    - Initial conditions

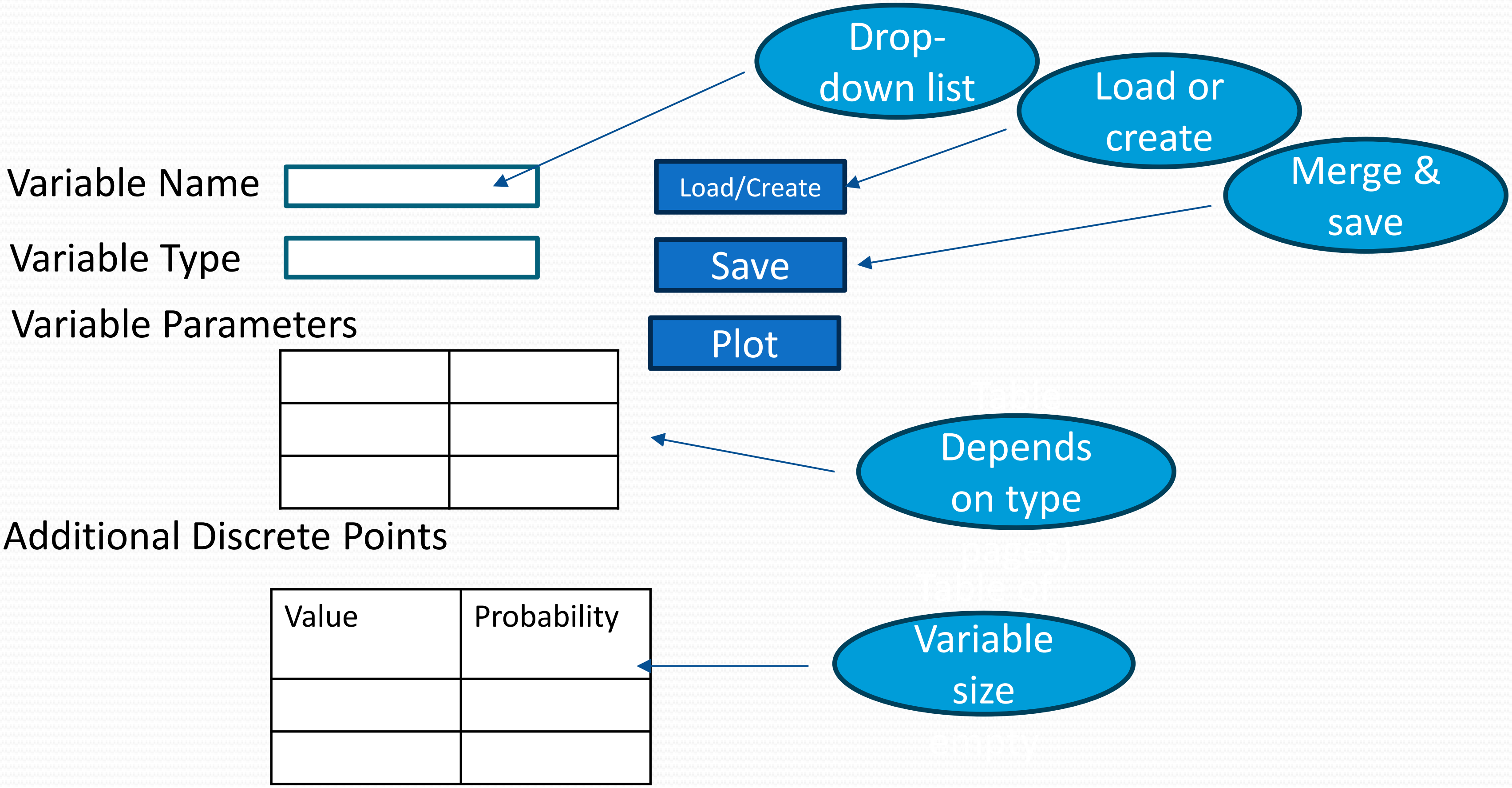
PDF Library

- Timeline tasks modeled as sequence of events
- Start times and durations modeled as random variables with defined probability density functions (pdfs)
- Resource consumption, command failures, etc also modeled as random variables with defined pdfs
- pdfs can be tailored prior to execution of monte carlo runs used to generate event lists

PDF Class

- Type – string
- Basic parameters – list depending on Type
- Additional points – list of tuples (value, probability) for edge cases, points of interest
- Lookup table populated from Type, Basic parameters, Additional points
- Method to populate Lookup table from Type, Basic parameters, Additional points
- Method to return a single random value from Lookup table

Creating/Editing pdf



Drop-down list

Load or create

Merge & save

Variable Name

Variable Type

Load/Create

Save

Plot

Variable Parameters

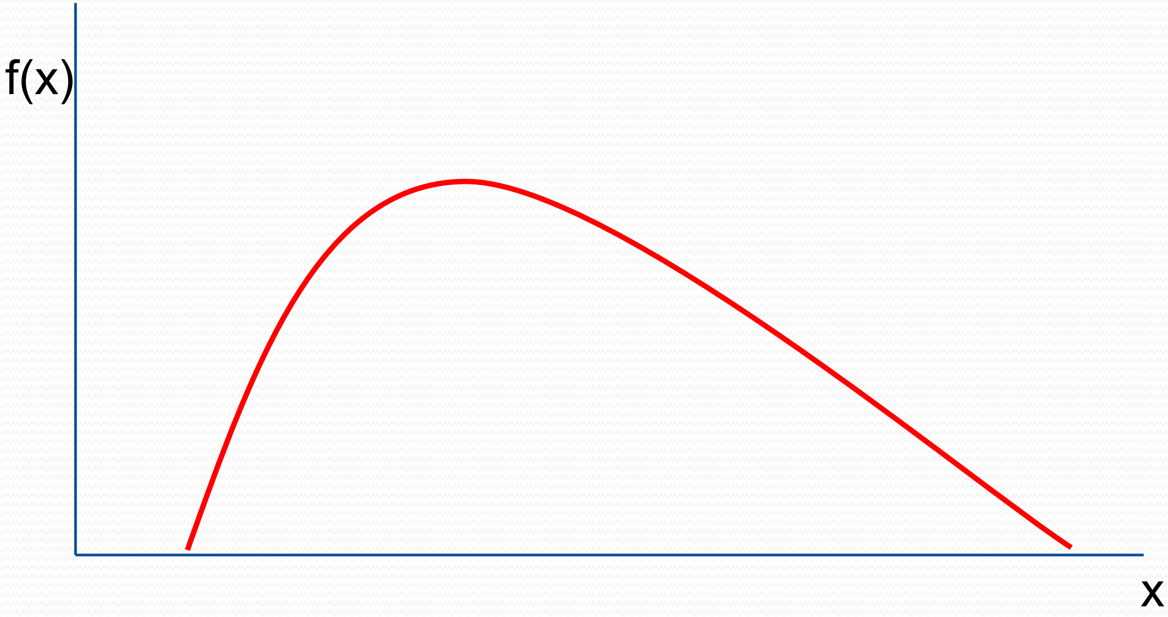
Depends on type

Additional Discrete Points

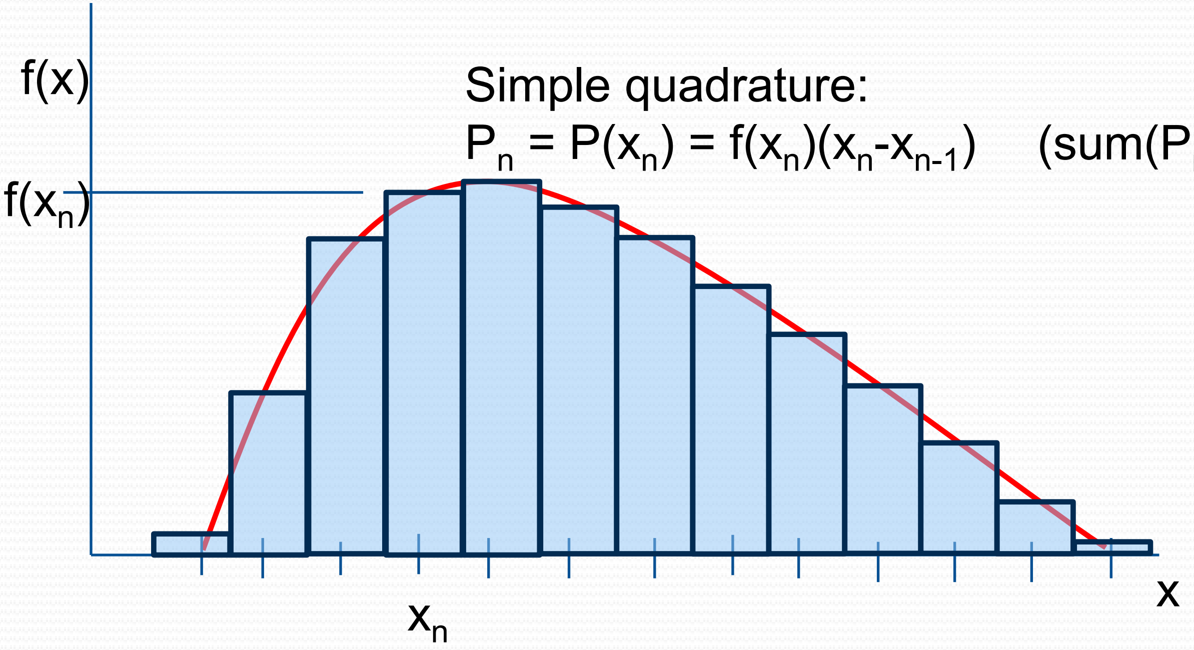
Value	Probability

Variable size

Example pdf Function



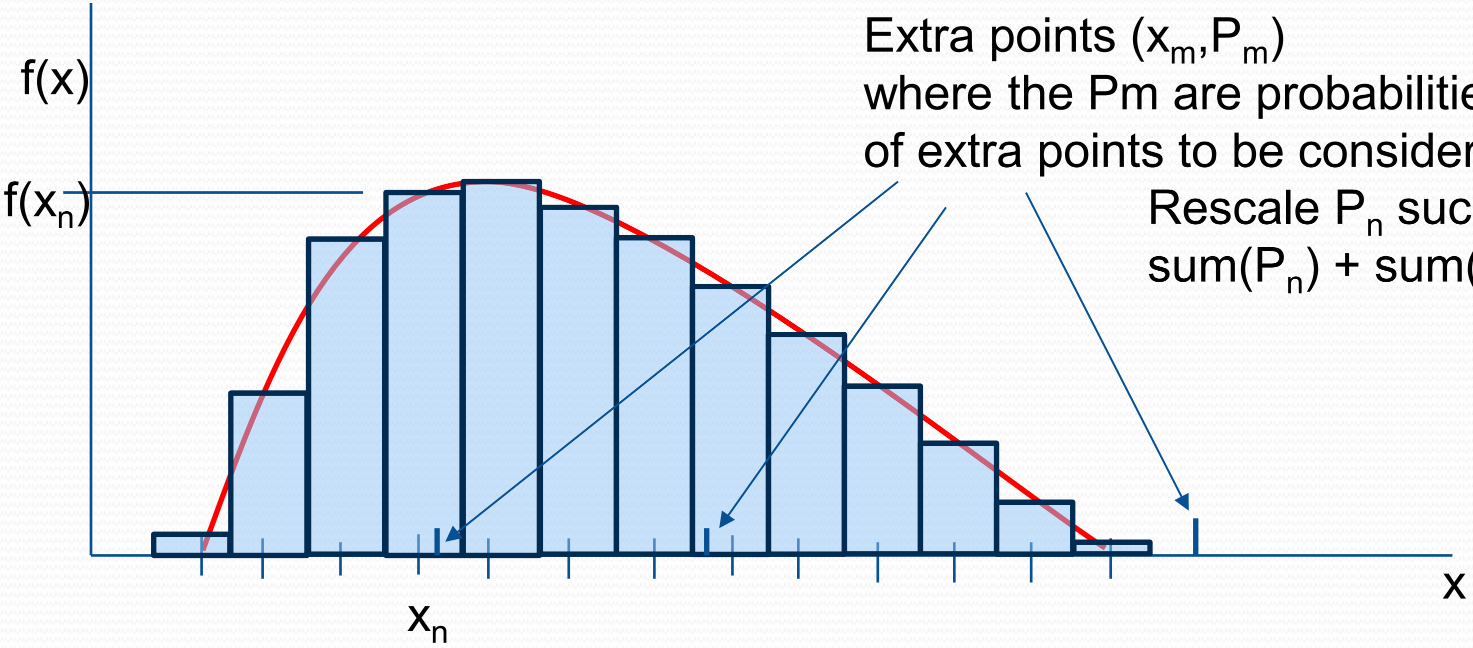
Bin the pdf Function



Simple quadrature:

$P_n = P(x_n) = f(x_n)(x_n - x_{n-1})$ (sum(P_n)=1)

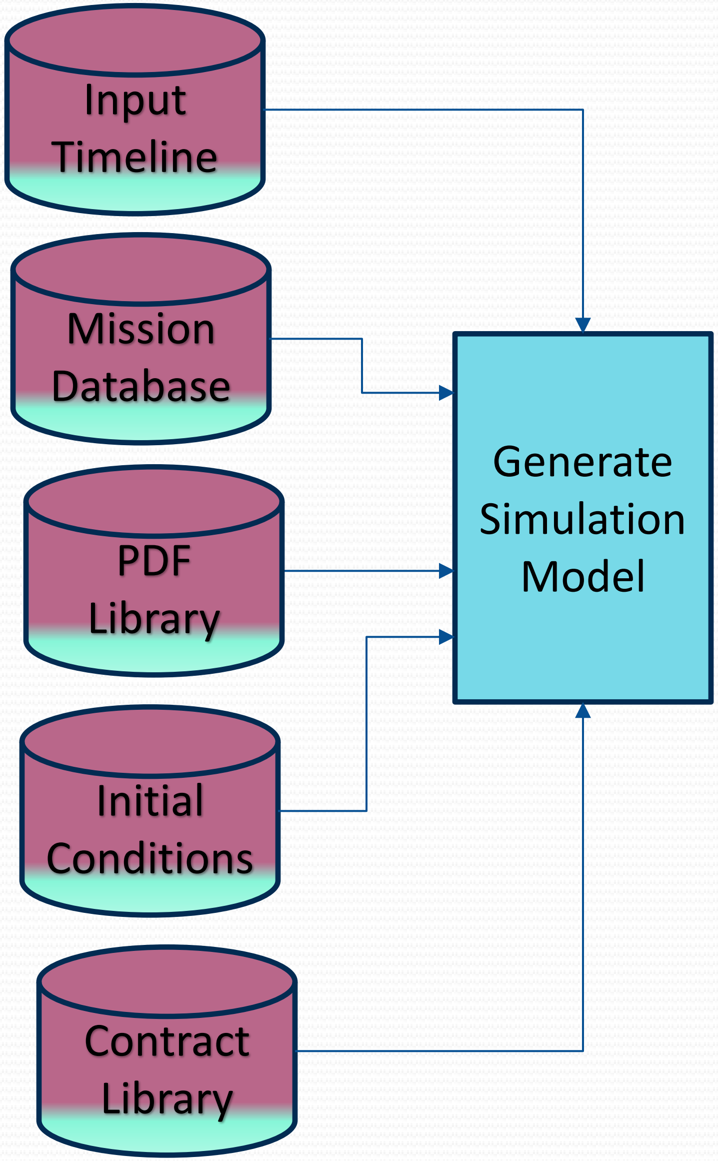
Add the extra points (corner cases, etc)



Extra points (x_m,P_m)
where the Pm are probabilities (small)
of extra points to be considered

Rescale P_n such that
$\text{sum}(P_n) + \text{sum}(P_m) = 1$

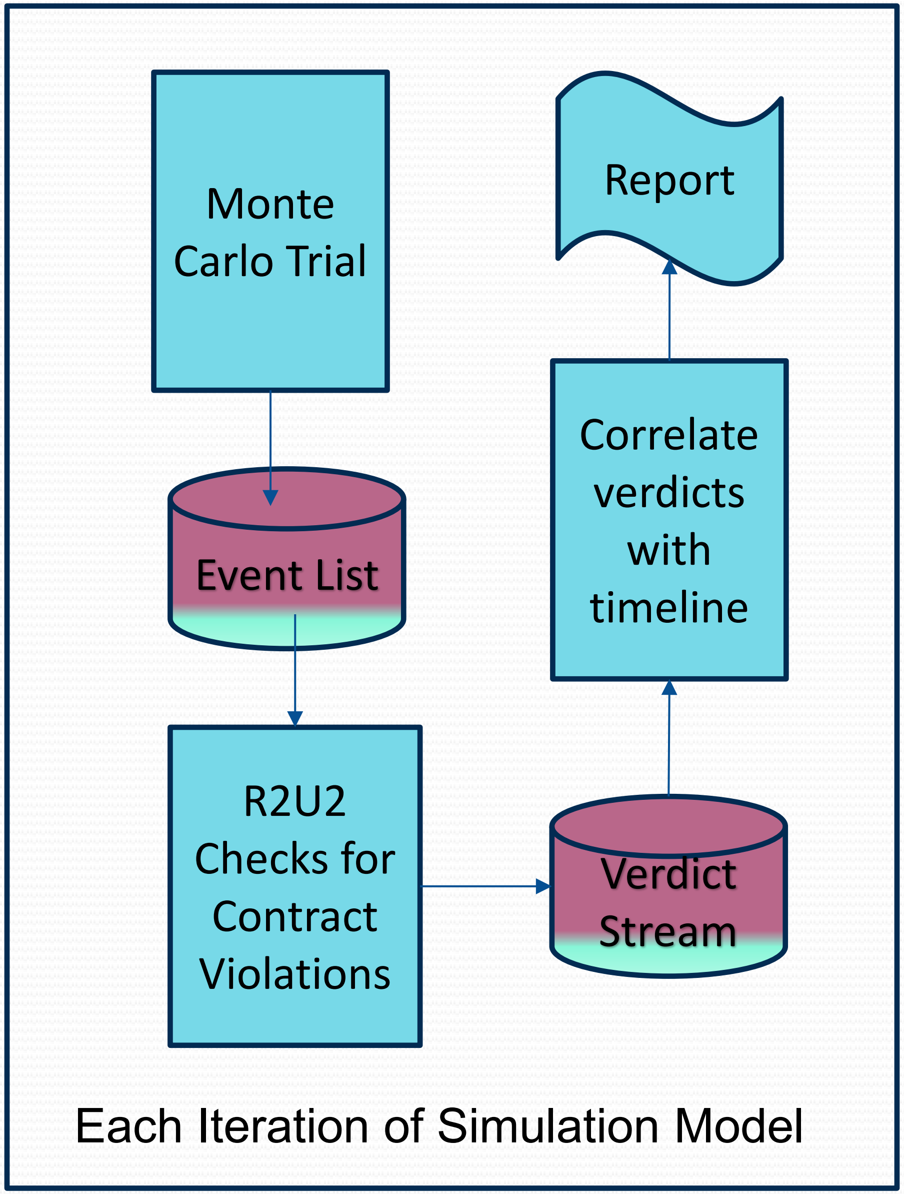
Simulation Model



- Class populated for a specific timeline
- Streamlined to permit rapid evaluation of each trial

Stochastic Validation Flow

- Each iteration produces event list data structure
- Event list converted by R2U2 into telemetry stream
- R2U2 model-checks
- Verdict stream converted into report


Monte Carlo Trial
Event List
R2U2 Checks for Contract Violations
Verdict Stream
Correlate verdicts with timeline
Report
Each Iteration of Simulation Model

Event List Data Structure

- Event list from each trial
  - Sequence of time-tagged events sorted by time of occurrence
  - Stepping by events ensures that something happens each step
  - Event lists is non-uniform in time
- Event list includes metadata to permit back-tracing to task which caused event

Stream Conversion for R2U2

- R2U2 designed to operate on telemetry stream with uniform time steps
- Assume-guarantee contracts written in MLTL which uses finite time brackets
- The R2U2 team at Iowa State University implemented a stream transformation and correctness proofs which permits trusted validation

Verdict Stream Reporting

- Realistic timelines result in thousands of verdicts per trial
- Primary interest is in failed verdicts
- Reporting tools
  - Display where in event list verdict failures occur
  - Trace failure events back to specific timeline task
  - Display trends, clusters
  - Visually isolate singular failures

Lessons Learned & Future Work

- The efficient generation of Monte Carlo timeline executions using the event list approach is viable
- The team found the automatic generation of assume-guarantee contracts to be straightforward
- Interfacing the event-list generation with R2U2 validation was successful due to close cooperation with ISU research team
- Improved results visualization tools will facilitate data interpretation