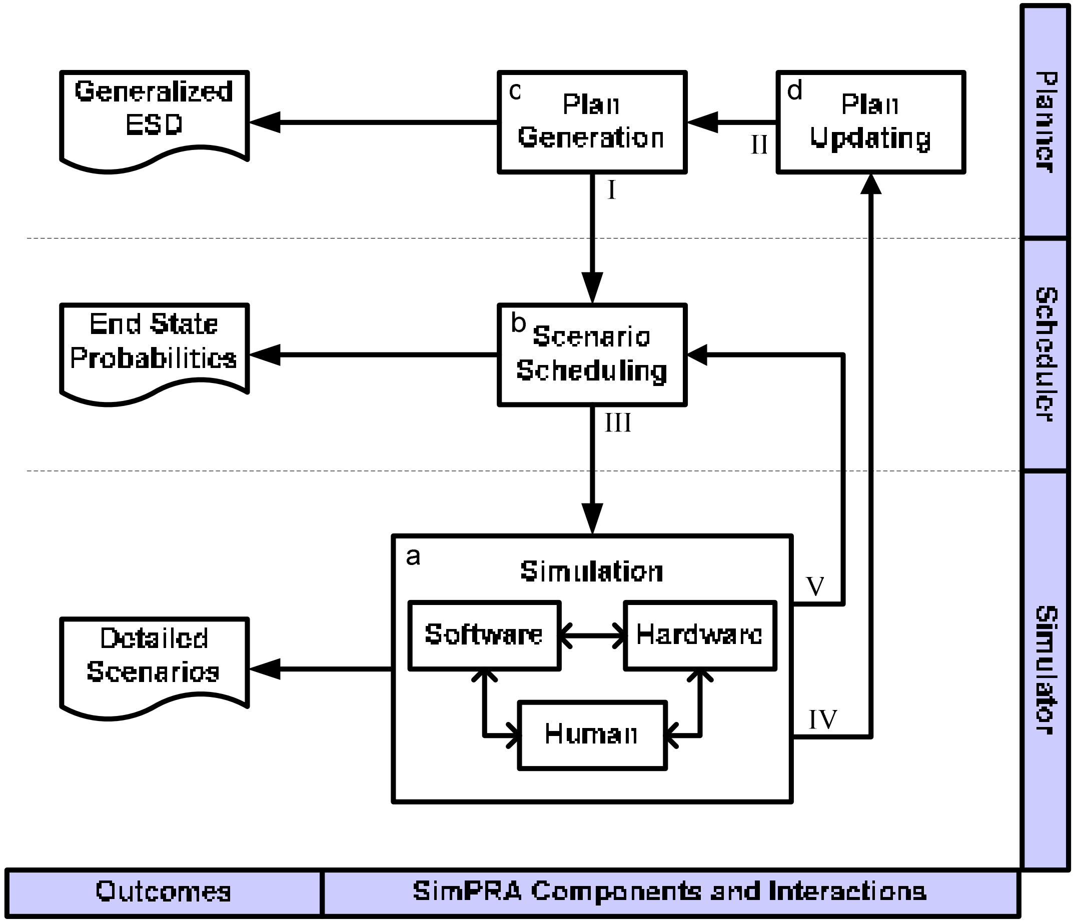
SimPRA: A Simulation-Based Probabilistic Risk Assessment Framework for Dynamic Systems

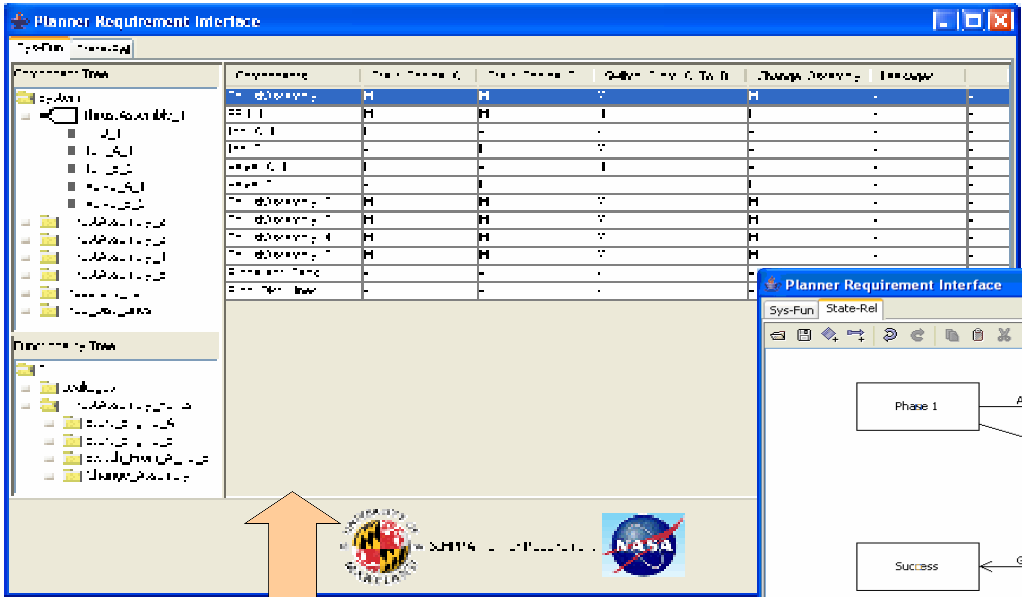
Ali Mosleh and Hamed Nejad
University of Maryland, College Park, MD

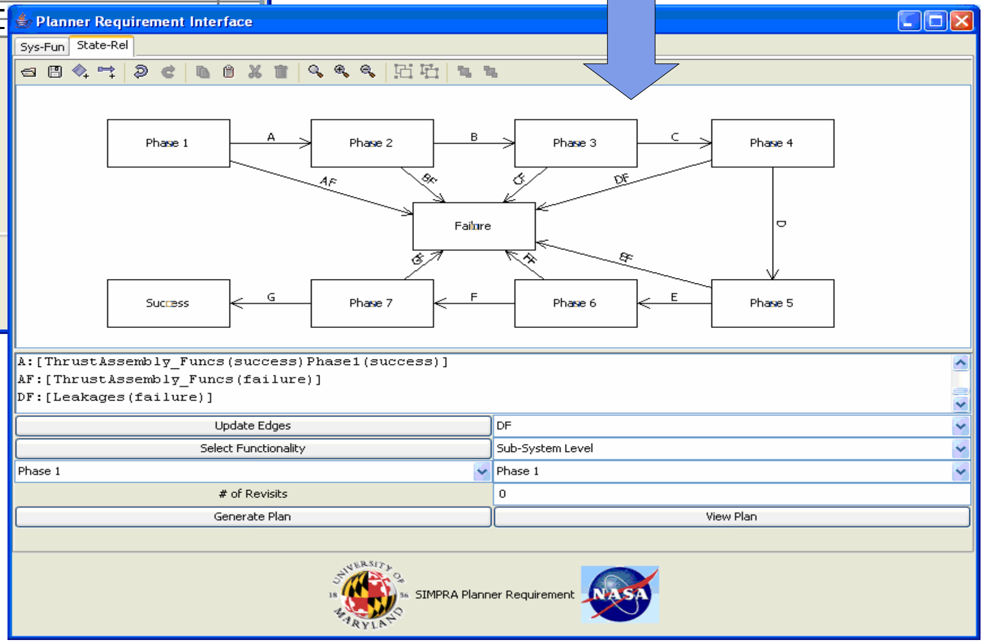
SimPRA – Simulation-based Probabilistic Risk Assessment Overview



Knowledge Capture
Simulation Planner Functions

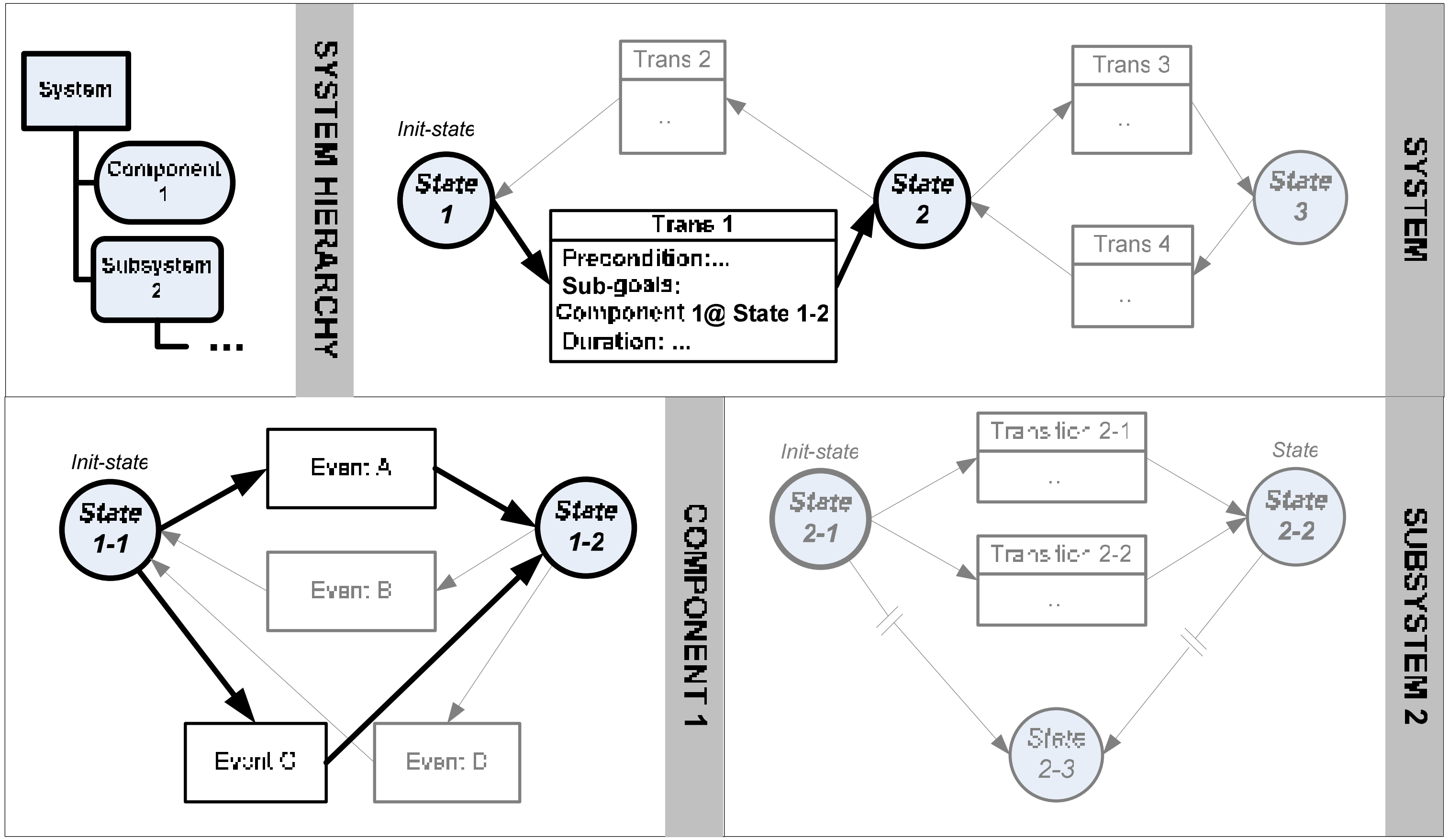
Hierarchical System State Modeling



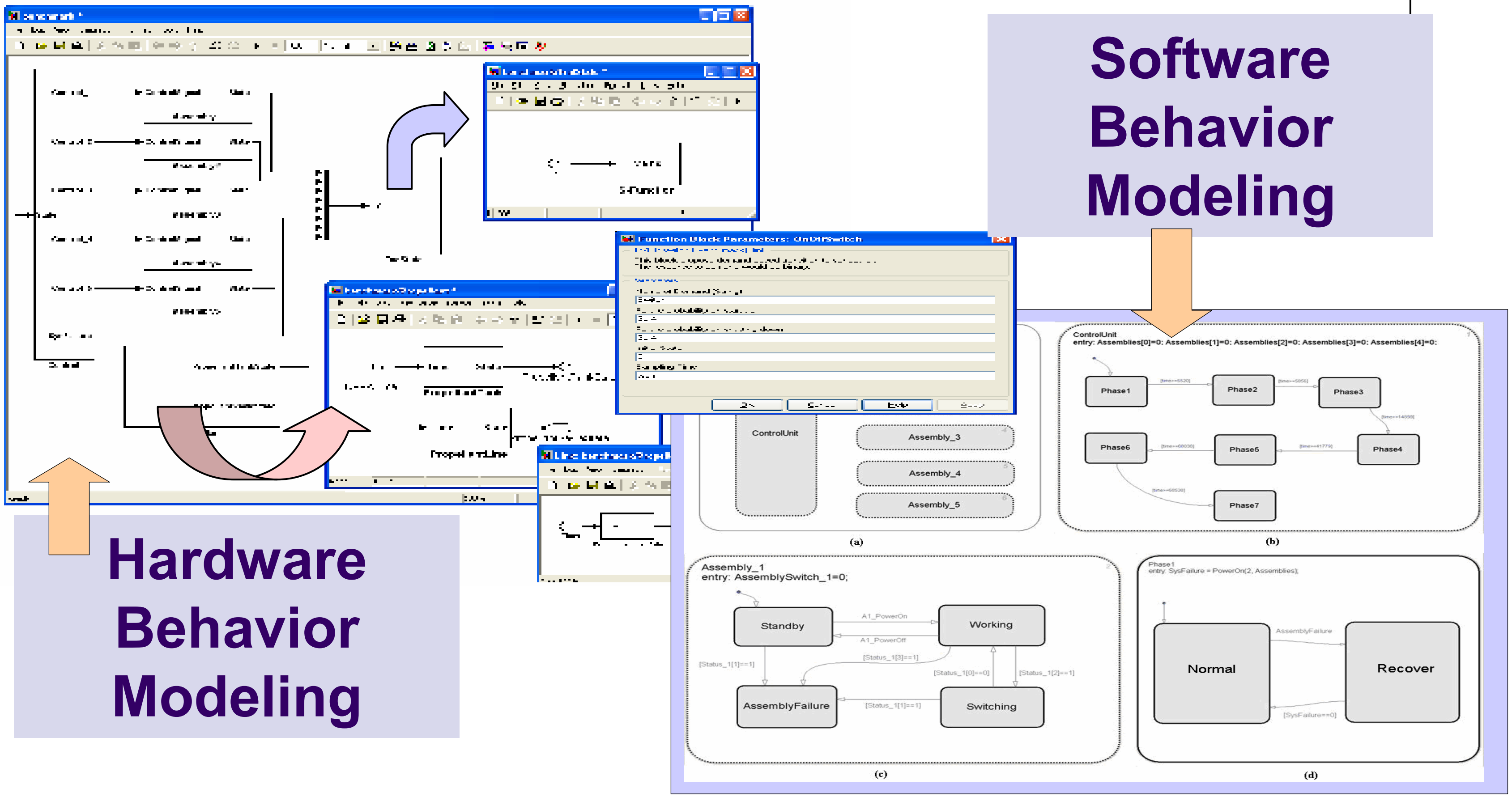


System Function-Structure Interdependencies

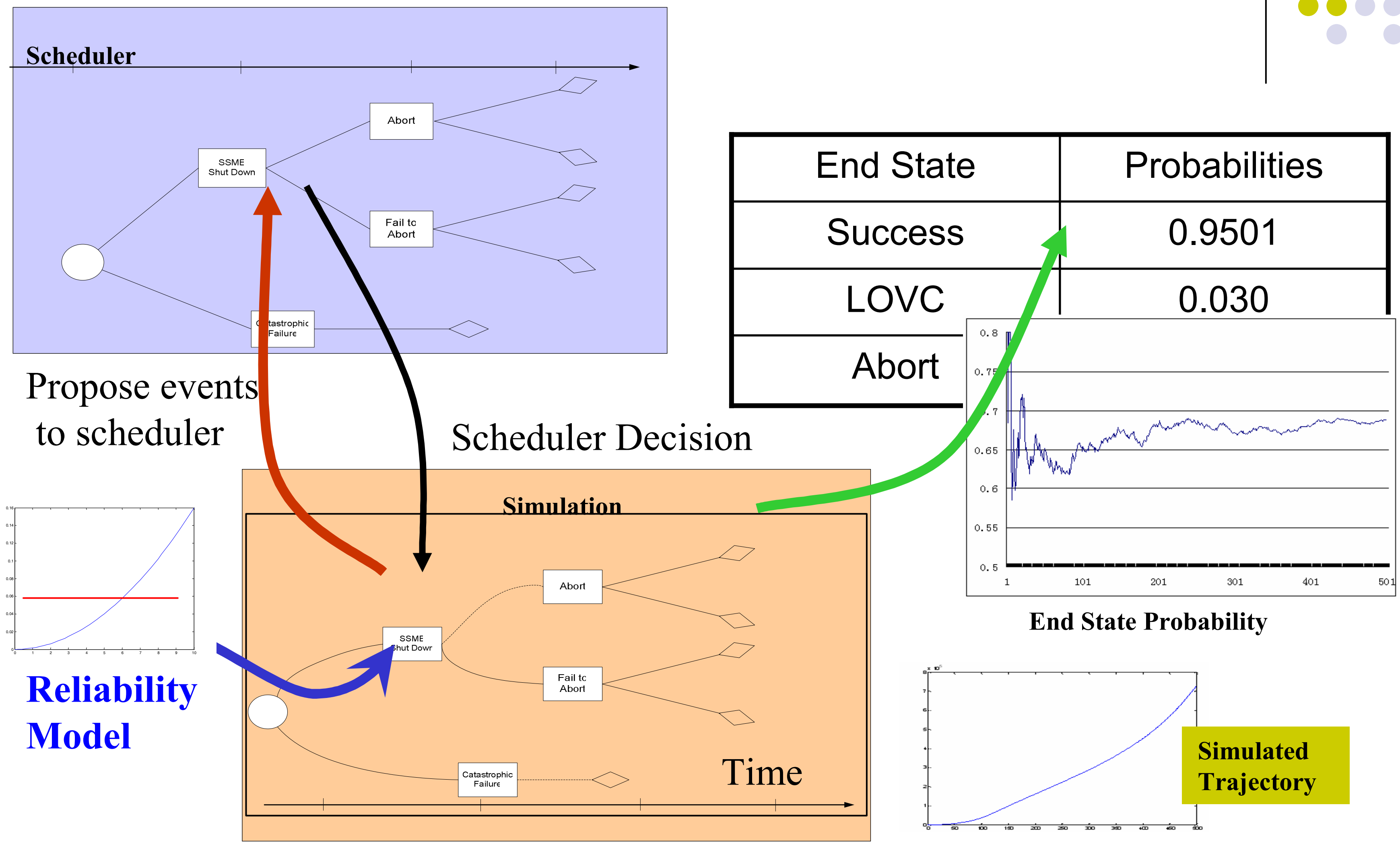
Hierarchical State Space Planner Model



Simulation Model Building (Probabilistic)



Scheduler- Simulator Interactions



End State	Probabilities
Success	0.9501
LOVC	0.030
Abort	[illegible]

SimPRA planner

- Captures high level engineering knowledge to provide high level scenarios for guiding the simulation.

  improves low probability high consequence scenario generation

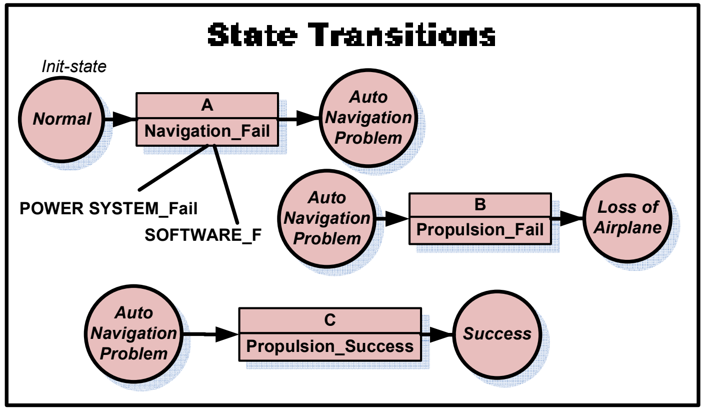
  helps simulation to converge to real probabilities faster
- Groups the scenarios to generate a complete picture of event sequences.

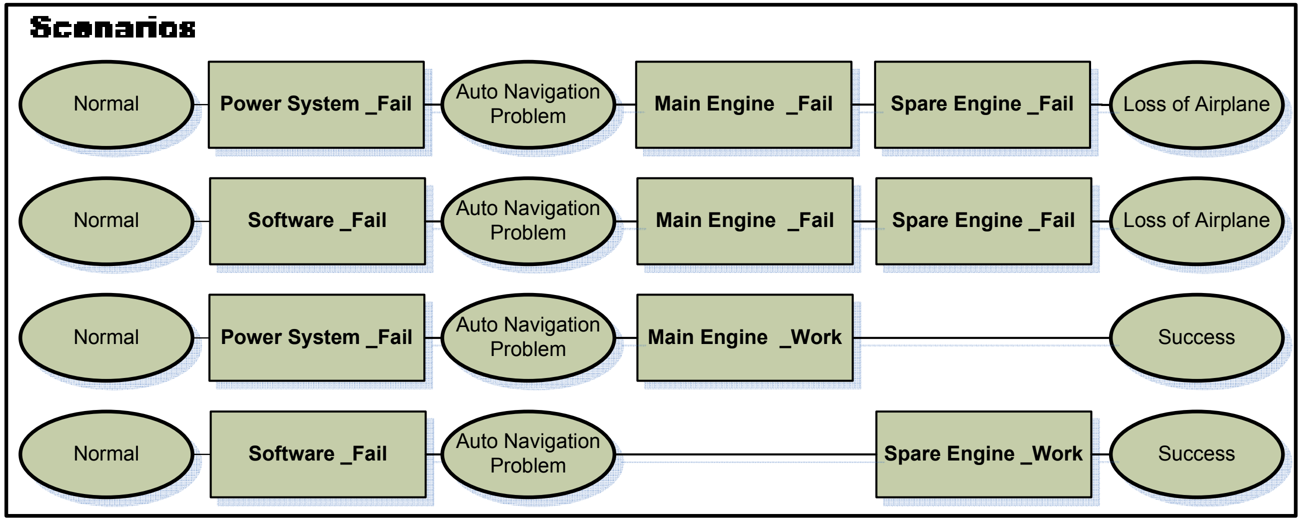
  ESD scenario representation for risk analysts
- Provides an environment that progressively improves the high level model over time.

Planning Example

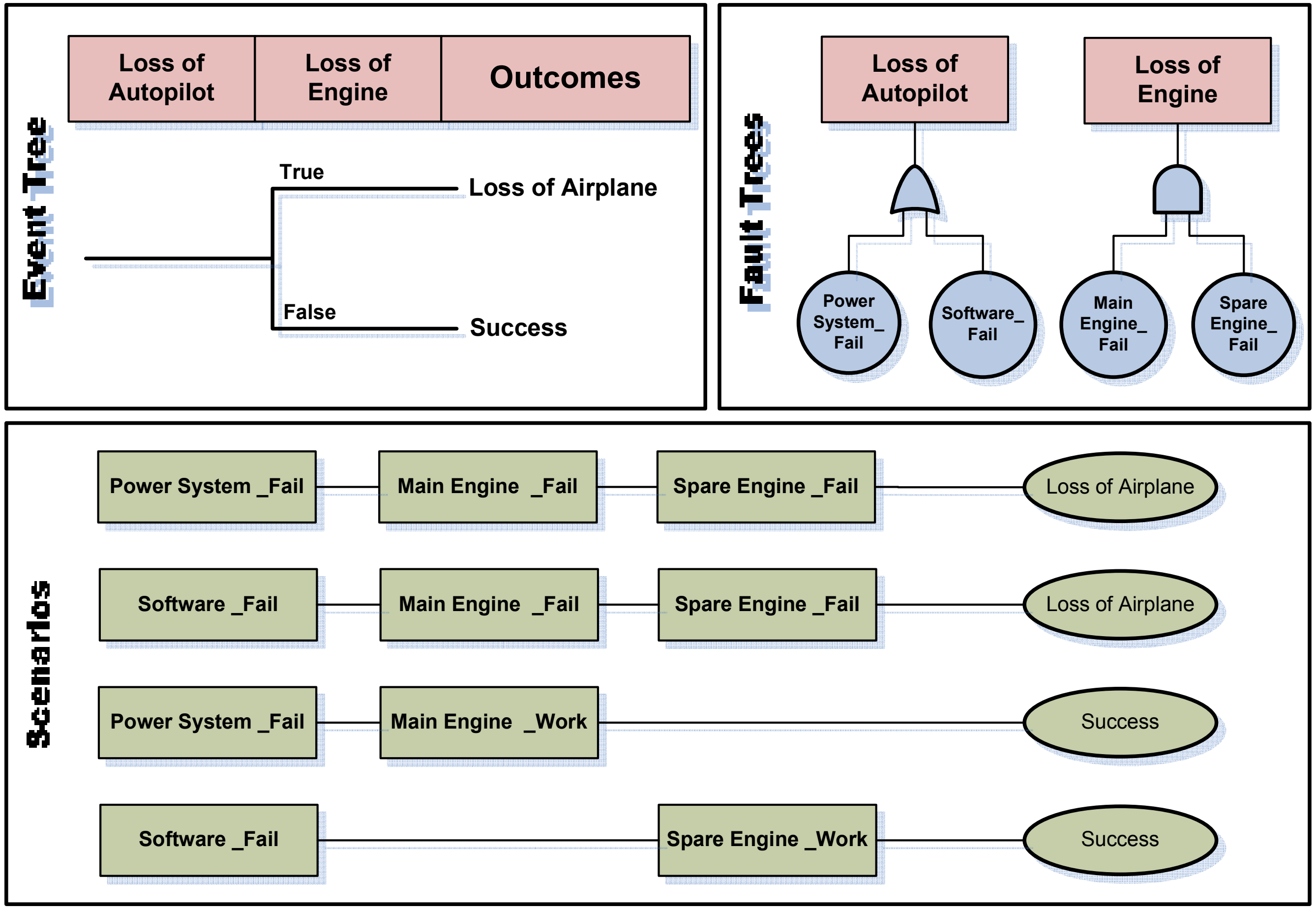
Component-Functionality Matrix

Component \ Functionality	Navigation	Propulsion
AUTOPILOT	x	
POWER SYSTEM	x	
SOFTWARE	x	
ENGINE		x
MAIN ENGINE		x
SPARE ENGINE		x





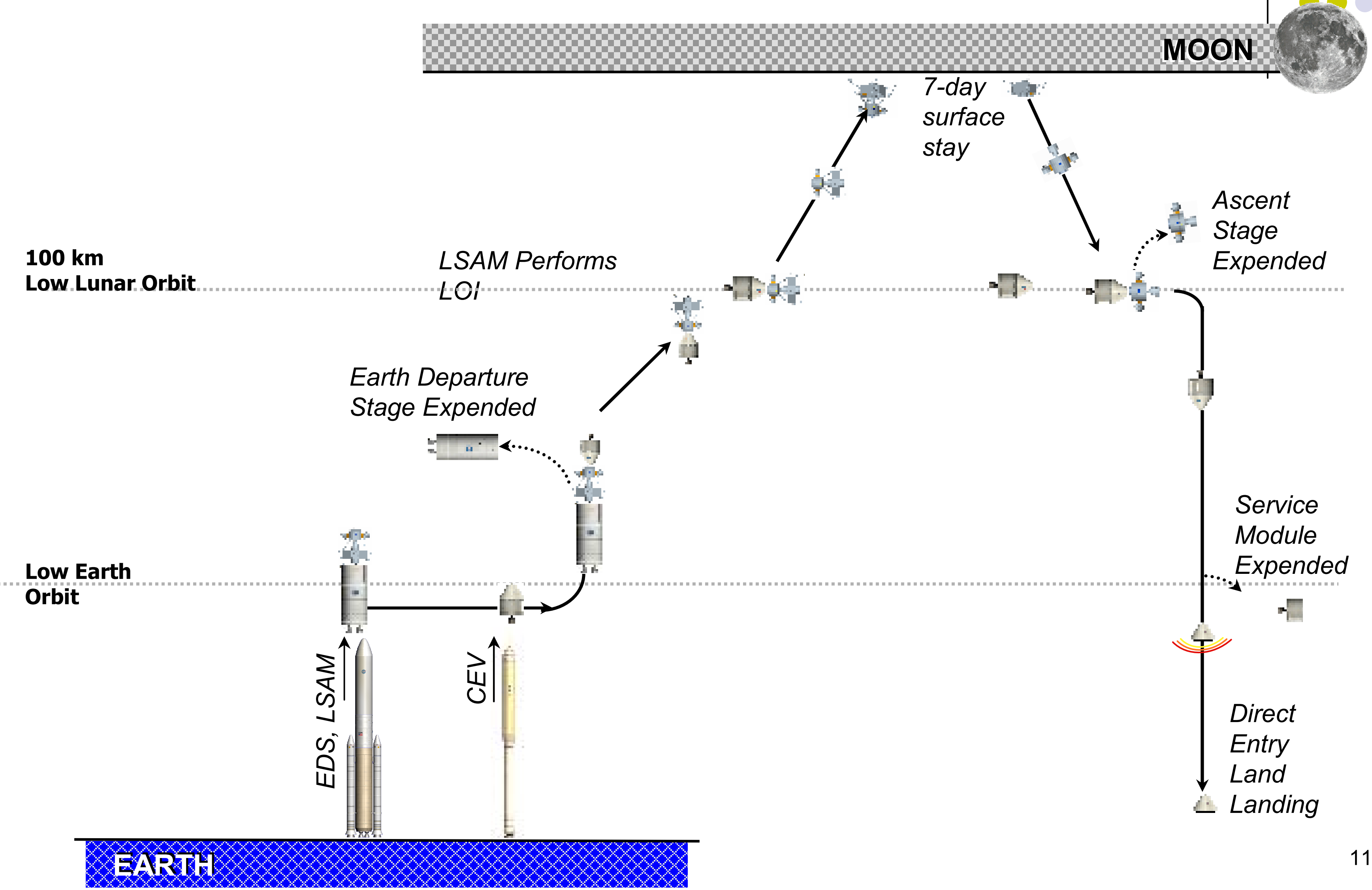
Comparison with FT/ET



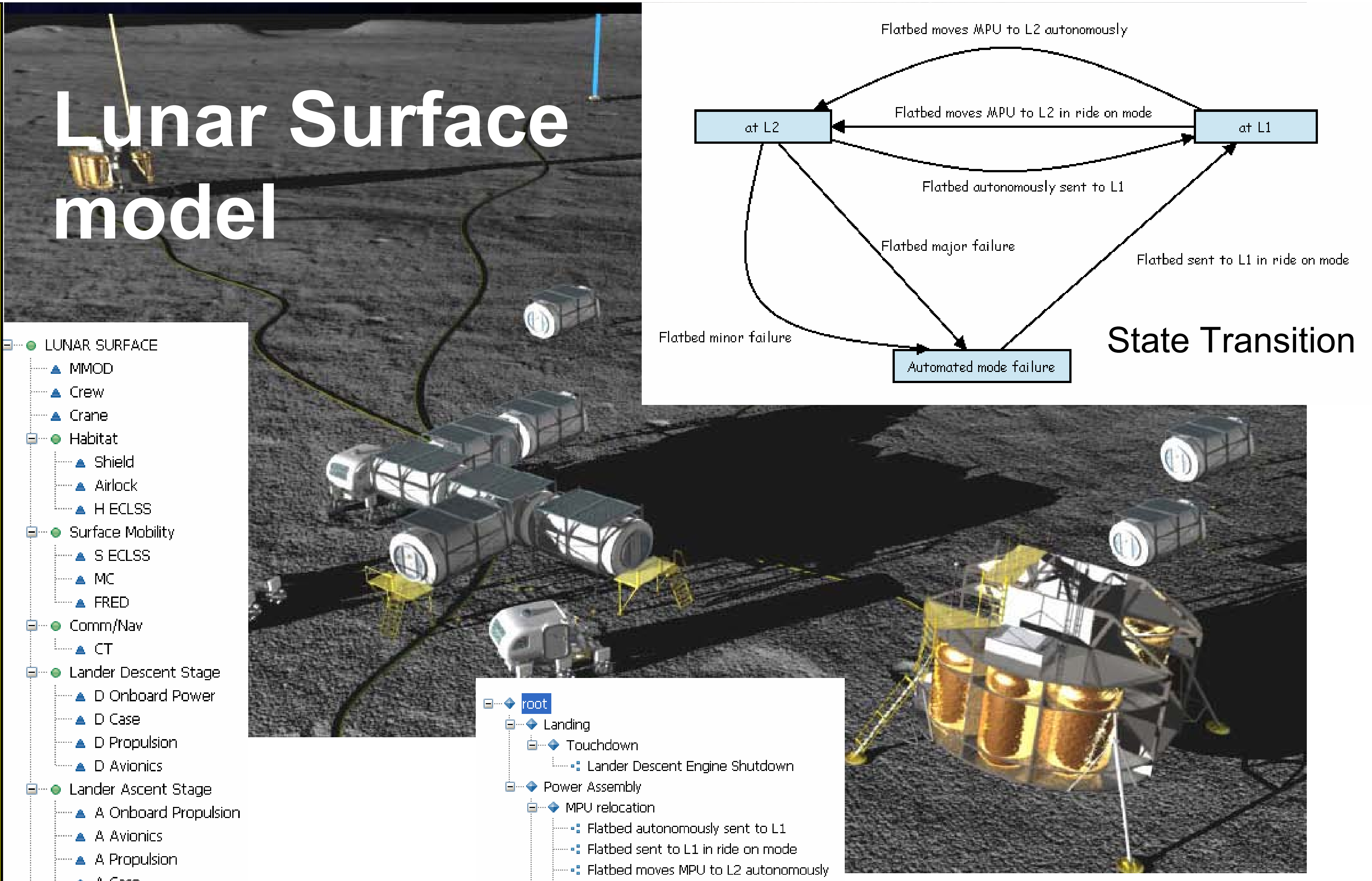
Binary vs Multi-state Planner

Type of Engineering Knowledge	Captured by	
	Binary planner	Multi-state planner
System elements and hierarchy	Structure Tree	Structure Tree
Elements' states and operational modes	Assumed binary (work or fail)	Structure Tree
Functionalities/ Activities/Events provided/Acted upon by elements	Functionalities for System level only	Functionality Tree
The relationship between functionalities and sub-functionalities/Activities and events	-	Functionality Tree
The allocation (assignment) of functionalities among components	Mapping between Functionalities and Structural Trees	Mapping between Functional and Structural Trees
The interplay between functionalities and states of the system	State Transition Diagram	State Transition Diagrams
The interplay between functionalities and states of the subsystems/ components	Assumed only one transition from work to fail state	State Transition Graphs
The relationship between the functionality of the system with the state of the subsystems and components	Mapping between Functionality Tree and Structure Tree	Transition Rules
Time dependencies	-	Transition Rules
Conditionality of the functionalities on the state of the other elements	-	Transition Rules
Importance of the elements to risk assessment	-	Transition Rules
Boundary conditions	Deducted from the Mapping between Functional and Structural Trees	Qualitative Reasoning Tree

Reference Lunar Sortie Mission



Lunar Surface model



State Transition

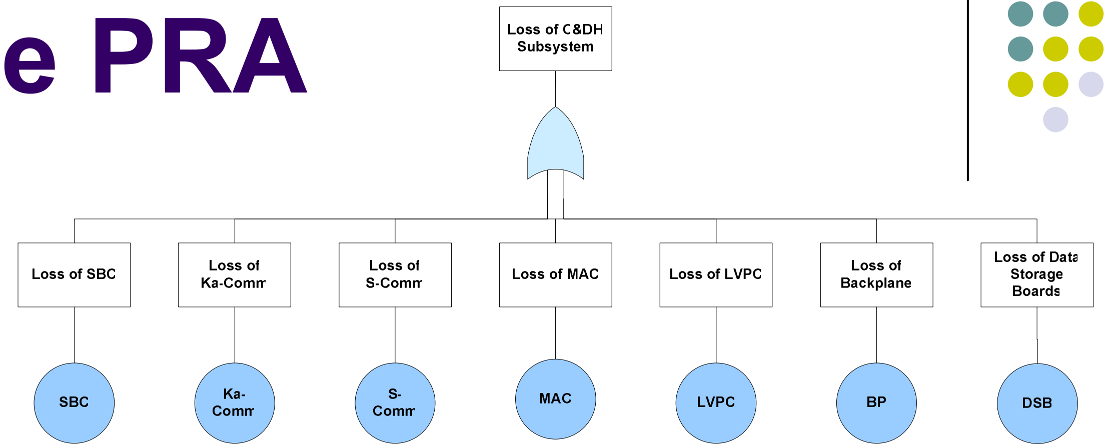
- LUNAR SURFACE
  - MMOD
  - Crew
  - Crane
  - Habitat
    - Shield
    - Airlock
    - H ECLSS
  - Surface Mobility
    - S ECLSS
    - MC
    - FRED
  - Comm/Nav
    - CT
  - Lander Descent Stage
    - D Onboard Power
    - D Case
    - D Propulsion
    - D Avionics
  - Lander Ascent Stage
    - A Onboard Propulsion
    - A Avionics
    - A Propulsion
    - A Case
    - L ECLSS
    - TCS
  - Power
    - SPU
    - MPU

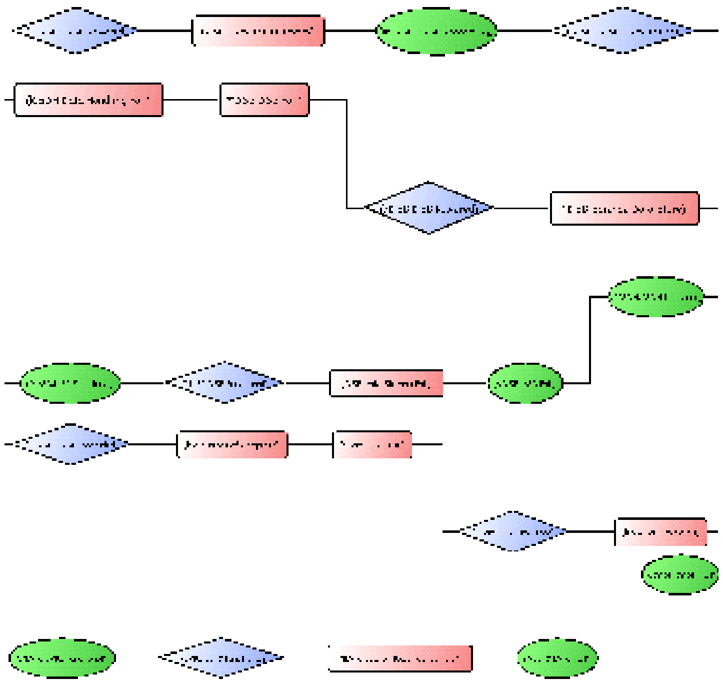
Structure Tree

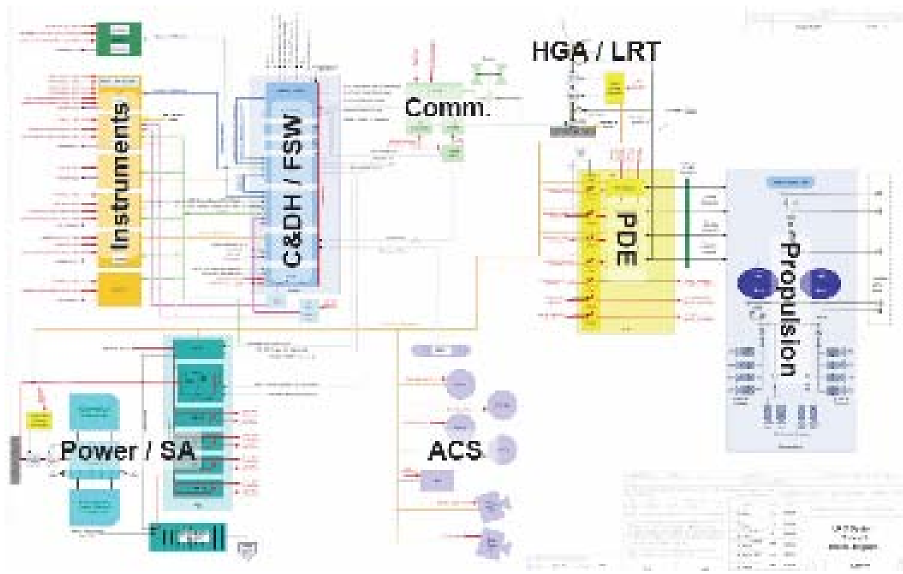
- root
  - Landing
    - Touchdown
      - Lander Descent Engine Shutdown
  - Power Assembly
    - MPU relocation
      - Flatbed autonomously sent to L1
      - Flatbed sent to L1 in ride on mode
      - Flatbed moves MPU to L2 autonomously
      - Flatbed moves MPU to L2 in ride on mode
    - LL connection to MPU
    - Assembly failure
      - Flatbed minor failure
      - Flatbed major failure
    - Assembly failure recovery
      - Crew EVA to L1
      - Crew EVA to L2

Functionality Tree

LRO Satellite PRA

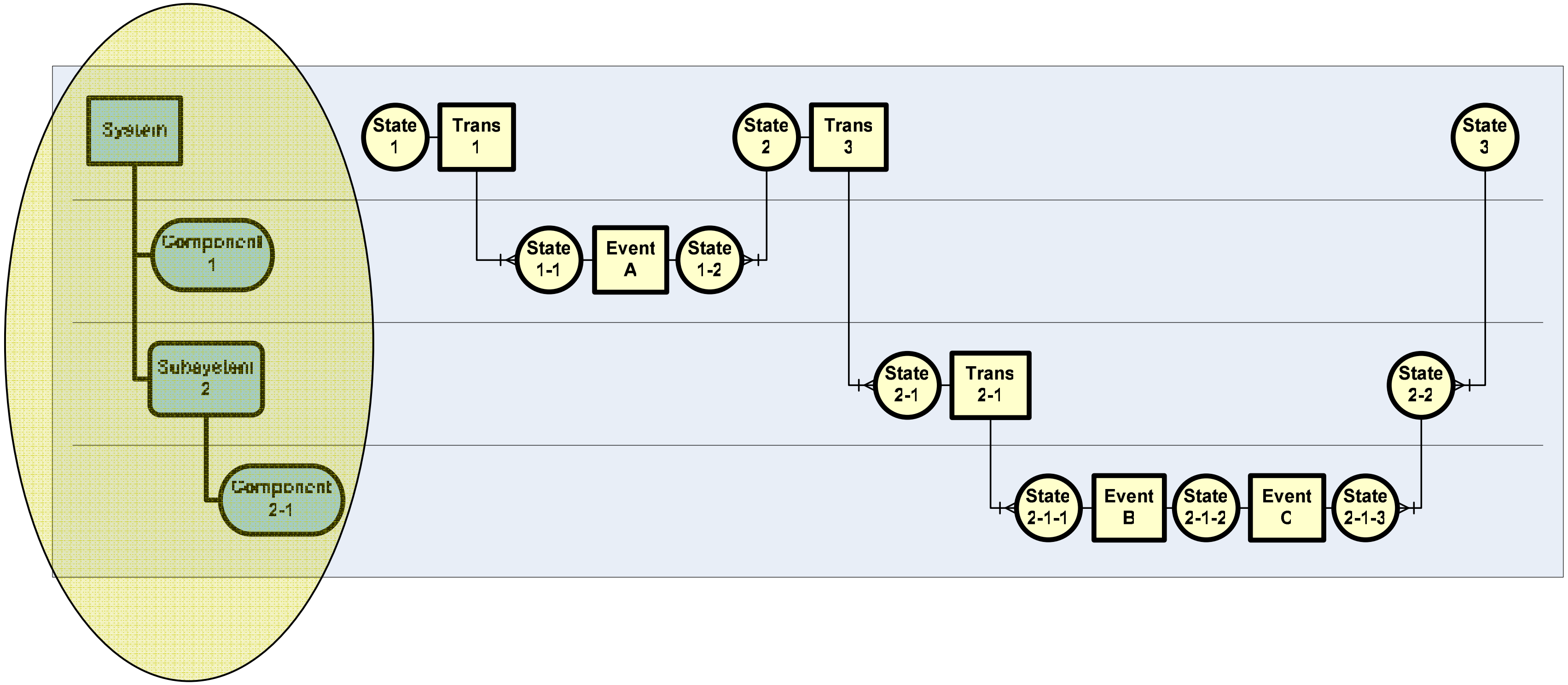






Introduction
SimPRA
Planner
Evaluation
RBD
Conclusion

Example of a Generated Plan (Event Sequence Diagram)



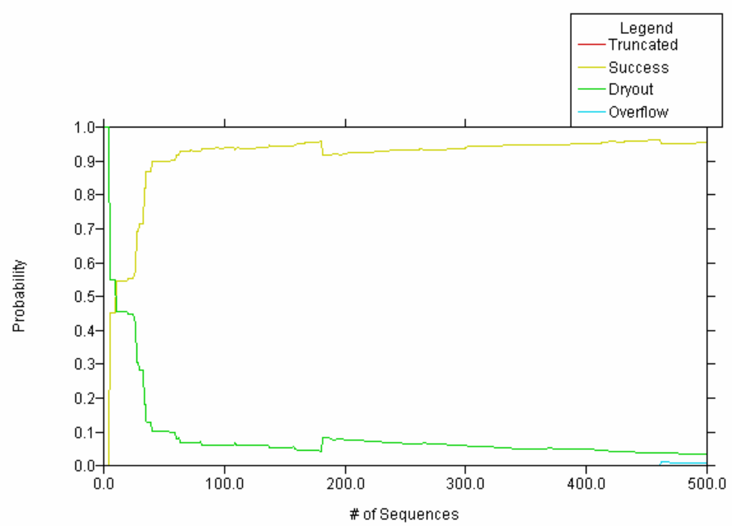
Plan Updating

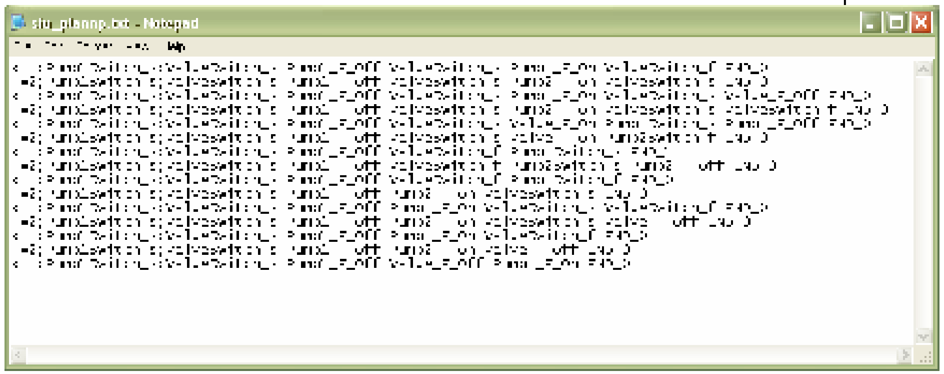
When a predefined number of simulation-runs are completed

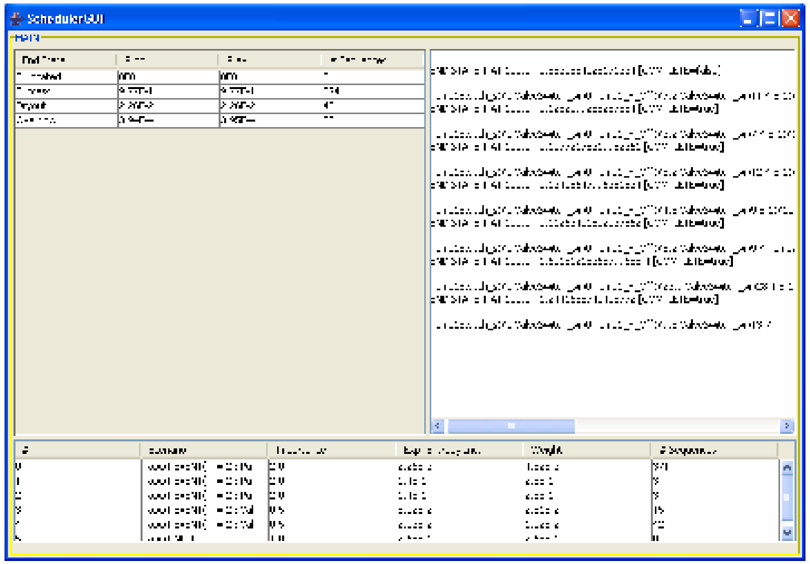
I. For components:
- checks every instance of a state change in the detailed scenarios
- if there is an event related to the component that is called between the changes of state, that event will be considered as the cause of the state transition for that component.
- If there is no event between state changes, then the previous event will be considered as the source of change for subsystems:
- ………..

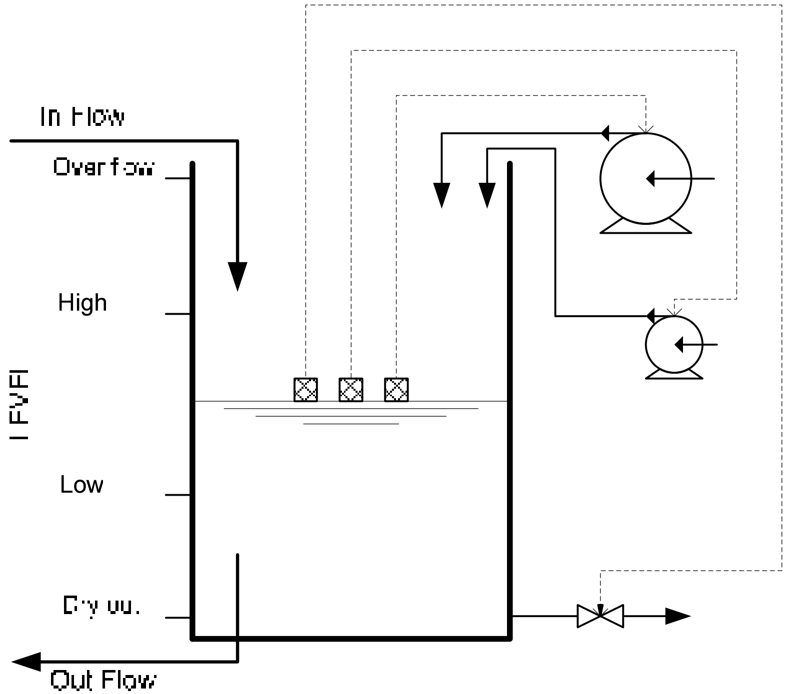
Simulation Log		Updater Output
#System:s1 > #Subsystem1:ss1 > #Comp1:c11 > #Comp2:c21 > !Comp1:event1 > !Comp2:event2 > #Comp2:c22 > #Comp1:c12 > #Comp1:c13 >#Subsystem1:ss2 > #System:s2	→	1: #Comp1:c11--> !Comp1:event1--> #Comp1:c12
		2: #Comp1:c12--> !Comp1:event1--> #Comp1:c13
		3: #Comp2:c21--> !Comp2:event2--> #Comp2:c22
		4: #Subsystem1:ss1--> @Comp1:c13 AND @Comp2:c22 --> #Subsystem1:ss2
		5: #System:s1--> @Subsystem1:ss2 --> #System:s2

Holdup tank example







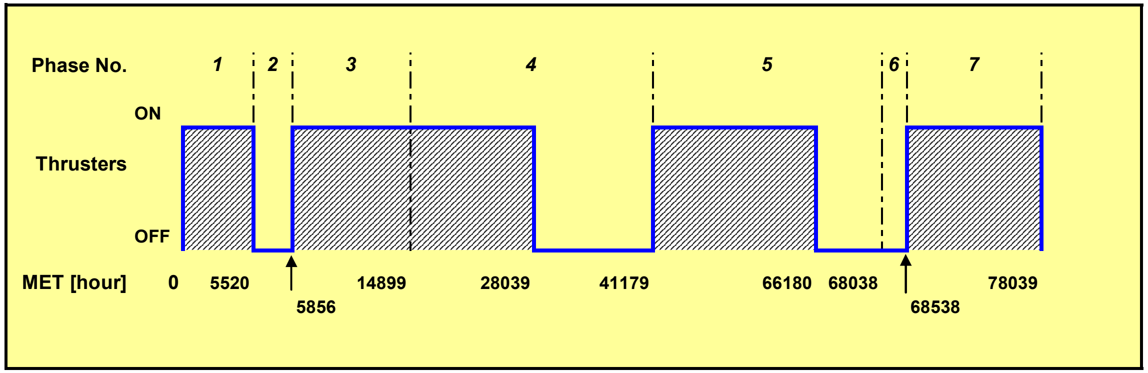


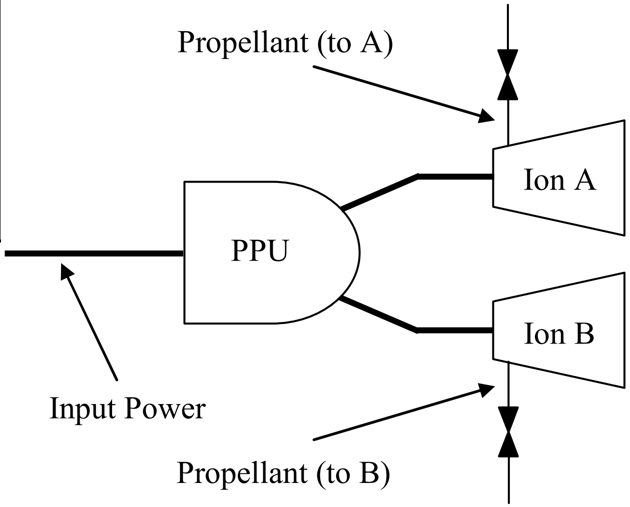
Holdup tank results

		Probability			SD	# Sequences		
		case 1	case 2	case 3		case 1	case 2	case 3
With Plan	Success	9.90E-01	9.88E-01	9.92E-01	2.00E-03	103	97	73
	Dry-out	9.73E-03	1.18E-02	7.88E-03	1.96E-03	350	353	371
	Overflow	9.02E-05	1.64E-04	1.39E-04	3.75E-05	47	50	56
Without Plan	Success	9.44E-01	9.53E-01	8.89E-01	3.46E-02	448	441	453
	Dry-out	5.57E-02	3.63E-02	9.87E-02	3.19E-02	27	35	26
	Overflow	4.88E-06	1.05E-02	1.25E-02	6.71E-03	25	24	21

- Low probability – High consequence scenarios are generated more often
- Since low prob scenarios get a place holder, simulation converges faster with plan

PSAM 8 Benchmark Problem

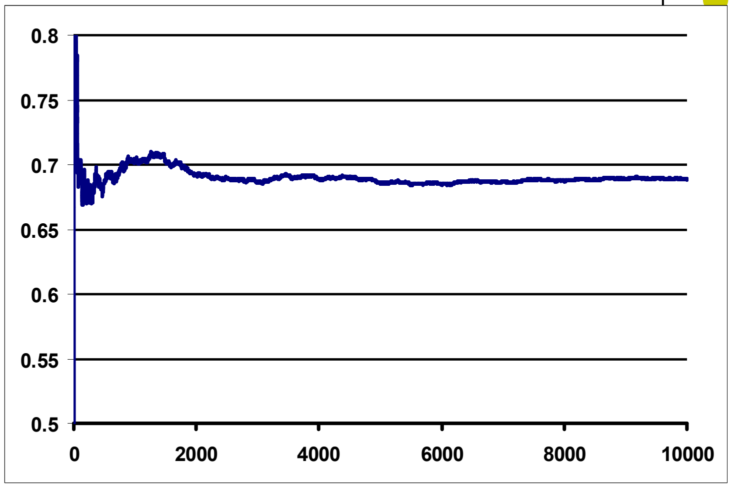




Component	Failure Mode	Effect
PPU	Fails to start on demand	Assembly failure
	Failure to operate	
	Failure to shutdown on demand	
Ion Engine A	Fails to start on demand	Loss of redundancy
	Failure to operate	
Ion Engine B	Fails to start on demand	Assembly failure
	Failure to operate	
Propellant Valve A	Failure to open on demand	Loss of Ion Engine A
	Failure to close on demand	System failure
	External leakage	
Propellant Valve B	Failure to open on demand	Loss of Ion Engine B
	Failure to close on demand	System failure
	External leakage	
Propellant tank	External leakage	System failure
Propellant distribution lines	External leakage	System failure

Group Size	Group Conditional Failure Probability [%]
2	8.0
3	4.0
4	2.0
5	1.0

Sample Result and Comparison



SimPRA Simulation

(500 runs)

Monte Carlo Simulation

(10000 runs)

Quantitative biasing (biased sampling)
Qualitative biasing (planning)
Dynamic Intelligent biasing (e.g., entropy based)

Primary Contributions

- A new method for capturing different types of engineering knowledge to automatically generate high level dynamic risk scenarios and
  - guide DPRA simulation
  - supply classical PRA techniques with generalized event sequence diagrams
  - a way to summarize simulation results for risk management
- As an integral element within the SimPRA framework, the planner has been shown to improve convergence and coverage of risk scenarios
- Computer implementation

Benchmark problem results

Name	Exact/ Approx. solution	Binary/ Multi state	Expandable	Low Prob. High Cons. Scenarios	Complex Systems	Common Cause	Demand-Based/ Time-Based	Model Complexity	Problem Solved
MC	Approximate	Binary but multi-state is also possible	Not known	No	Yes	Yes	Both	High	Yes [E-1]
DFM	Analytical	Binary	Yes	Yes	No	Not shown	Both	Can't get too complex	No
DFT	Exact	Binary	Yes	Yes	No	Not shown	Time based only	Not easy to develop	Yes but way too far of other solutions [E-13]
AO-MC	Approximate	Multi state	Yes but only horizontally	No	Yes	Yes	Both	Complex	Yes[E-1]
SAPHIRE	Exact	Multi state	In some cases in a static form	Yes	No	Yes	Both	Very hard to model	No
FT/ET/Markov	Analytical approach, approximate solutions	Multi state	No	Yes	No	Yes	Both	Not easy to develop	Yes but out of range solutions [E-3]
SimPRA	Approximate	Multi state	Yes, both horizontally and vertically	Yes	Yes	Yes	Both	Complex	Yes [E-1]
DES (TIGER)	Approximate	Multi state	Not known	Not known	Yes	Yes with difficulty	Time based. Demand based with difficulty	Not too complex	Yes [E-1]