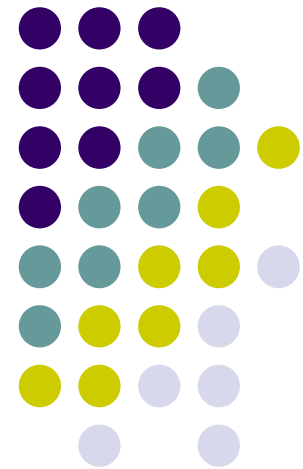
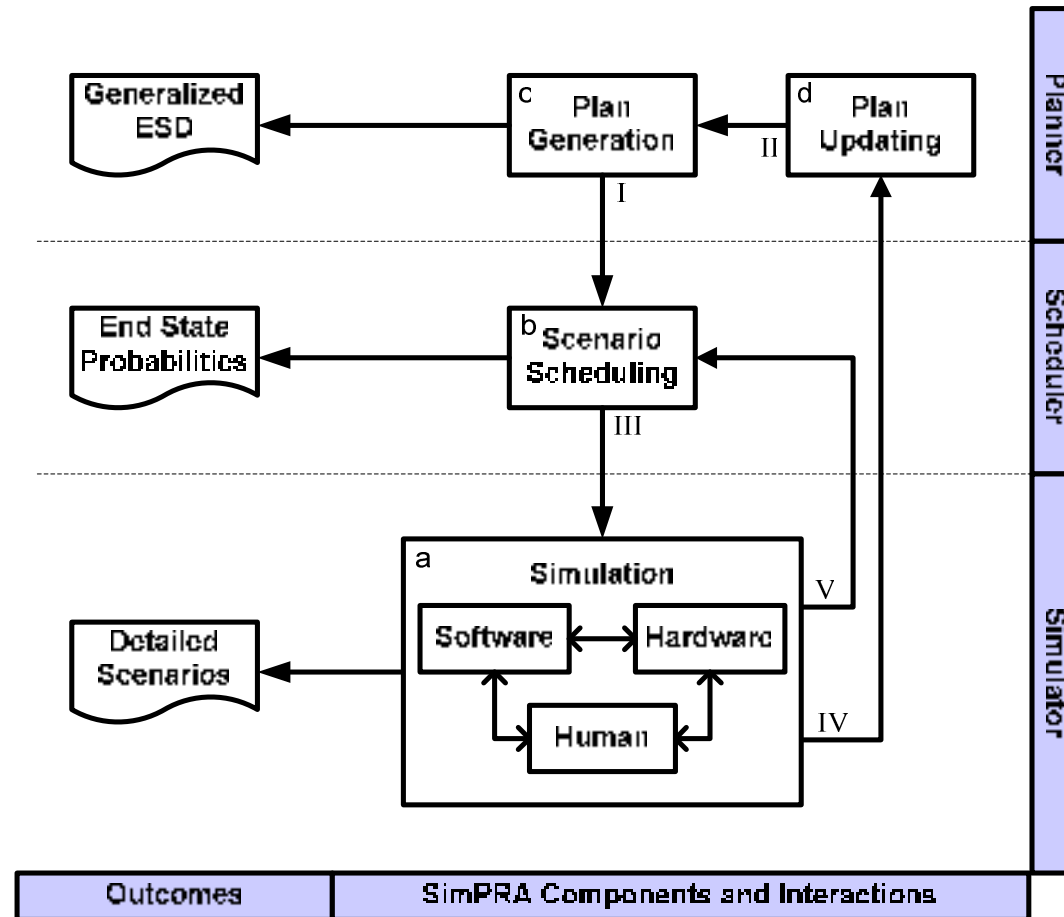


SimPRA: A Simulation-Based Probabilistic Risk Assessment Framework for Dynamic Systems

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**

Requirement ID	Requirement Name	Priority	Category	Phase	Start Time	End Time	Dependencies
R001	Thrust Assembly 1	H	M	Phase 1	0	10	
R002	Leakage 1	M	F	Phase 1	0	10	R001
R003	Thrust Assembly 2	H	M	Phase 2	10	20	R001
R004	Leakage 2	M	F	Phase 2	10	20	R003
R005	Thrust Assembly 3	H	M	Phase 3	20	30	R003, R004
R006	Leakage 3	M	F	Phase 3	20	30	R005
R007	Thrust Assembly 4	H	M	Phase 4	30	40	R005, R006
R008	Leakage 4	M	F	Phase 4	30	40	R007
R009	Thrust Assembly 5	H	M	Phase 5	40	50	R007, R008
R010	Leakage 5	M	F	Phase 5	40	50	R009
R011	Thrust Assembly 6	H	M	Phase 6	50	60	R009, R010
R012	Leakage 6	M	F	Phase 6	50	60	R011
R013	Thrust Assembly 7	H	M	Phase 7	60	70	R011, R012
R014	Leakage 7	M	F	Phase 7	60	70	R013

**System Function-
Structure
Interdependencies**

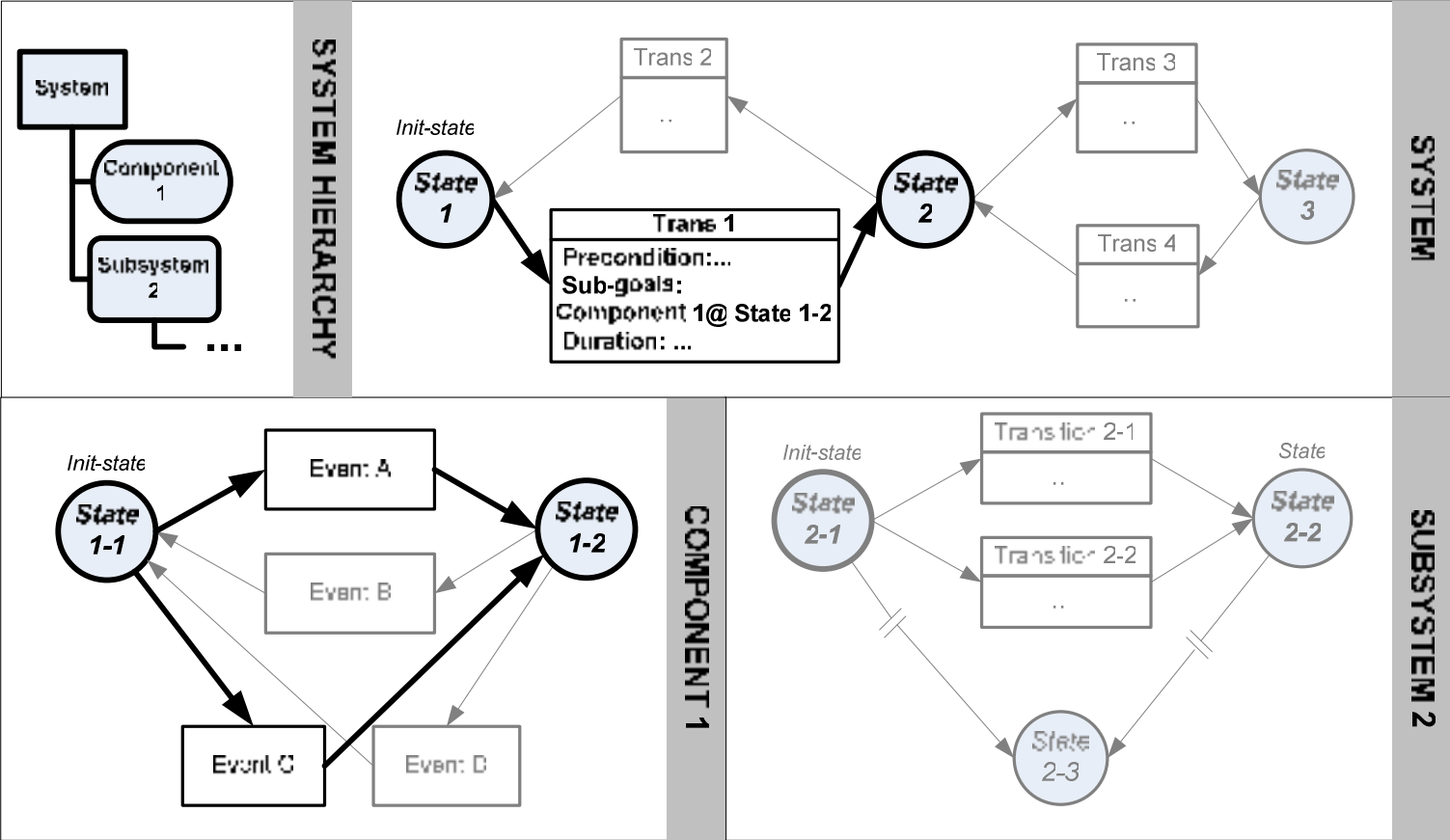
```

    graph LR
      Phase1[Phase 1] -- A --> Phase2[Phase 2]
      Phase1 -- AF --> Failure[Failure]
      Phase2 -- B --> Phase3[Phase 3]
      Phase2 -- BF --> Failure
      Phase3 -- C --> Phase4[Phase 4]
      Phase3 -- CF --> Failure
      Phase4 -- D --> Phase5[Phase 5]
      Phase4 -- DF --> Failure
      Phase5 -- E --> Phase6[Phase 6]
      Phase5 -- EF --> Failure
      Phase6 -- F --> Phase7[Phase 7]
      Phase6 -- FF --> Failure
      Phase7 -- G --> Success[Success]
      Phase7 -- GF --> Failure
  
```

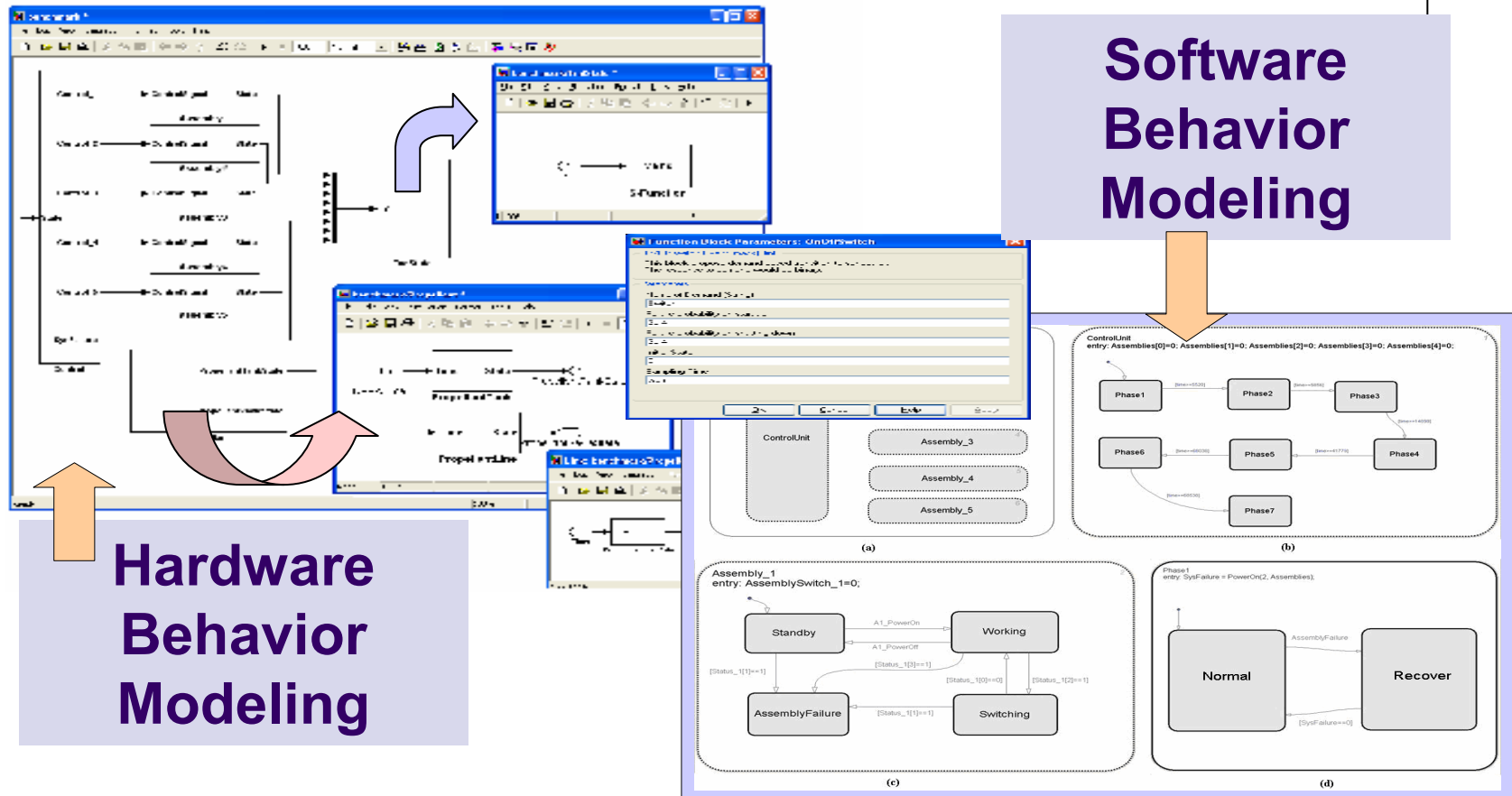
A: [ThrustAssembly_Funcs (success) Phase1 (success)]
 AF: [ThrustAssembly_Funcs (failure)]
 DF: [Leakages (failure)]

Update Edges: DF
 Select Functionality: Sub-System Level
 Phase 1: Phase 1
 # of Revisits: 0
 Generate Plan: View Plan

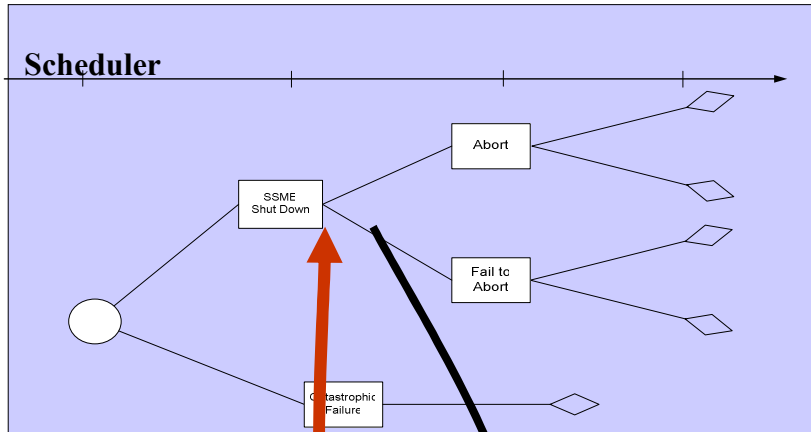
Hierarchical State Space Planner Model



Simulation Model Building (Probabilistic)



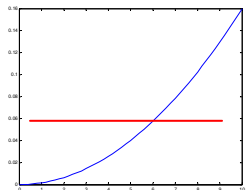
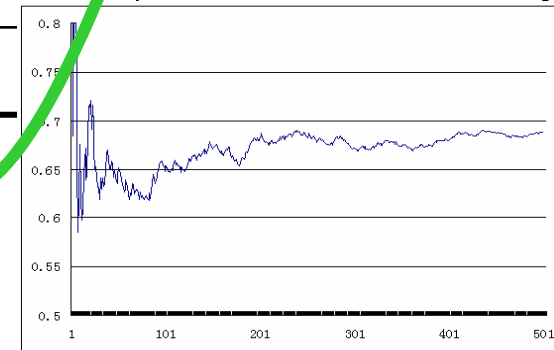
Scheduler- Simulator Interactions



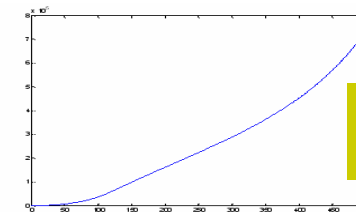
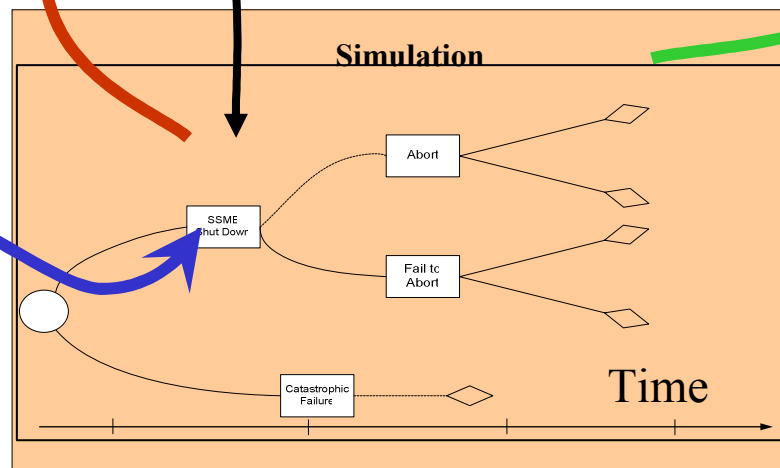
Propose events to scheduler

Scheduler Decision

End State	Probabilities
Success	0.9501
LOVC	0.030
Abort	



Reliability Model



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.

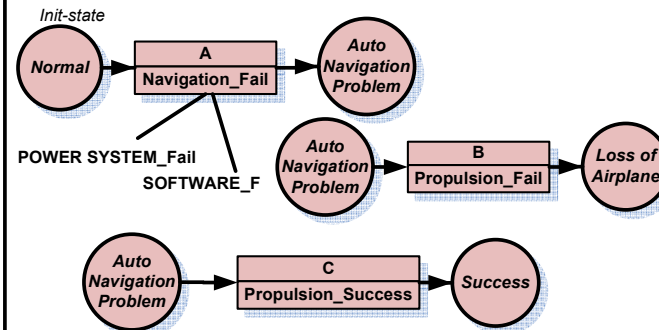
Planning Example



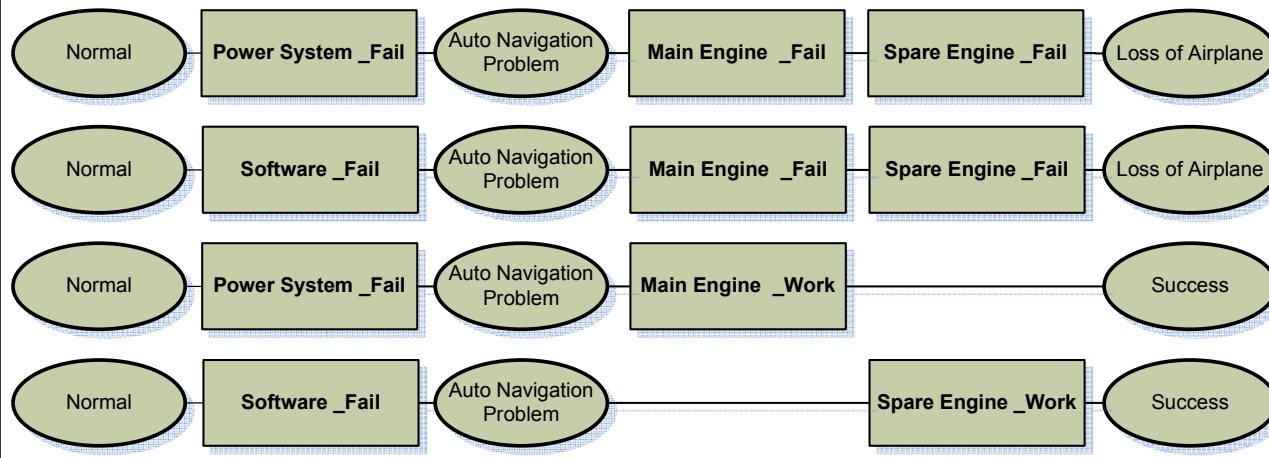
Component-Functionality Matrix

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

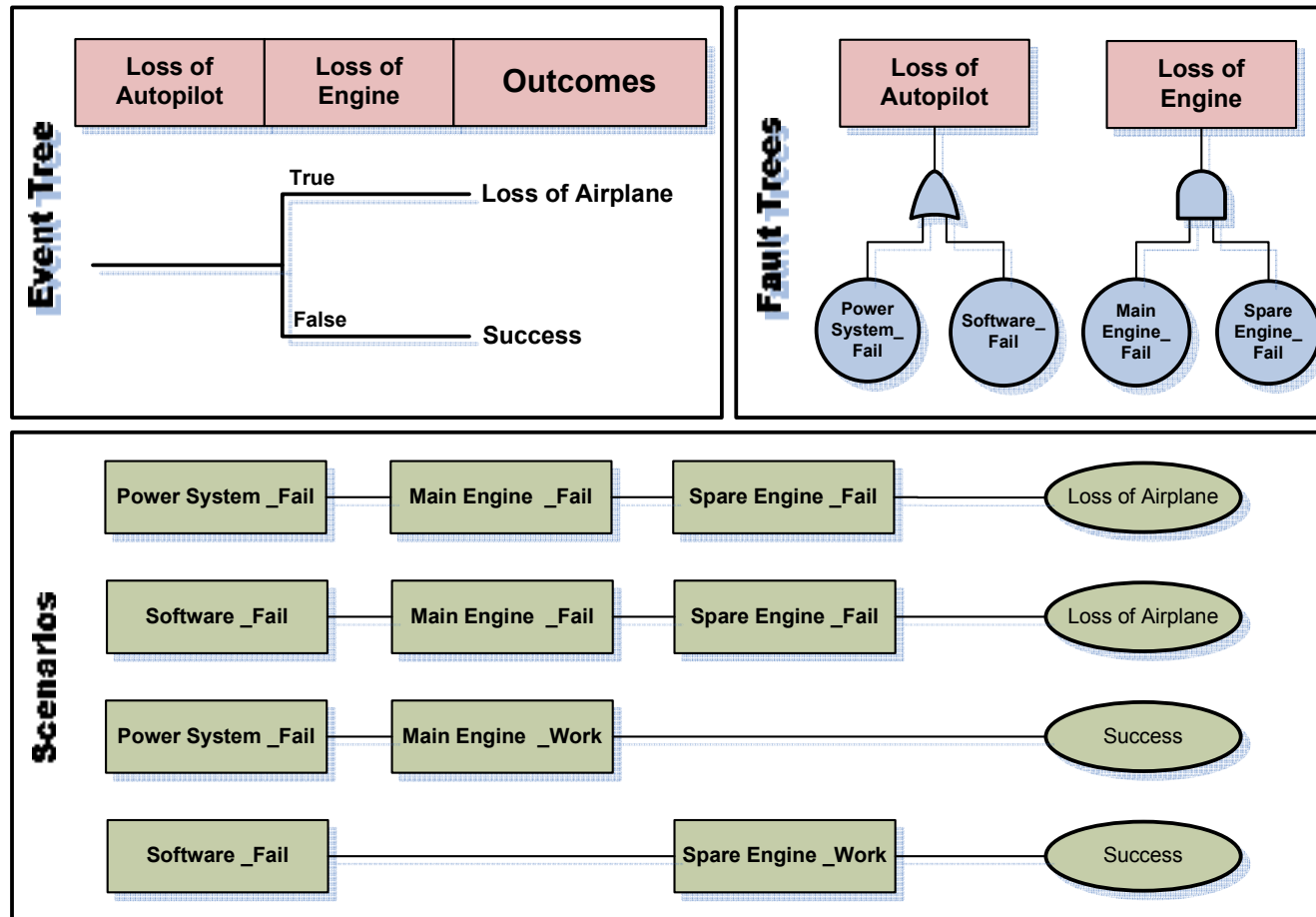
State Transitions



Scenarios



Comparison with FT/ET

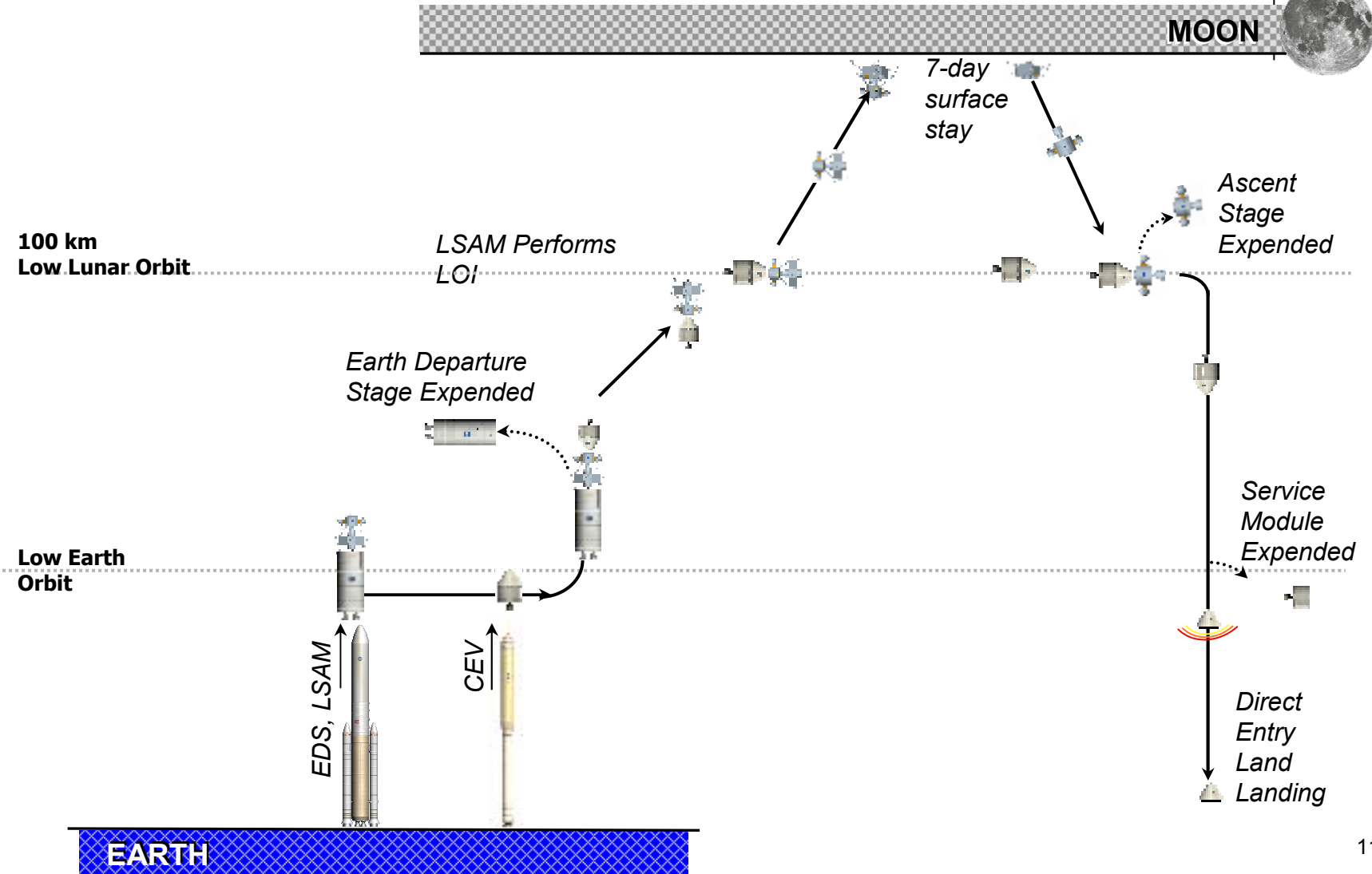


Binary vs Multi-state Planner

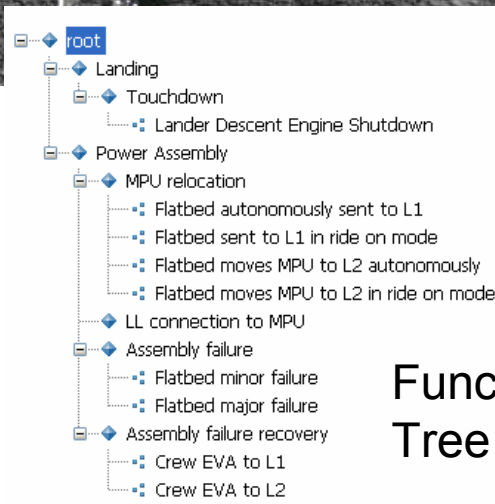
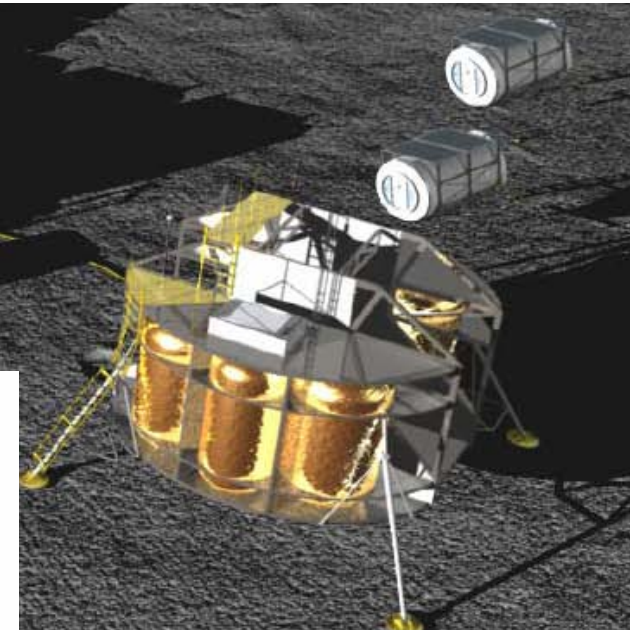
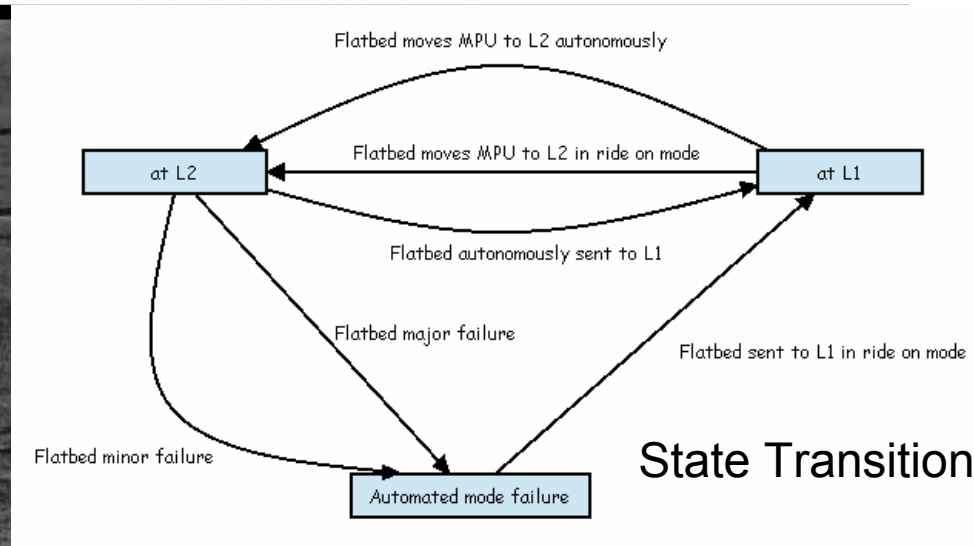
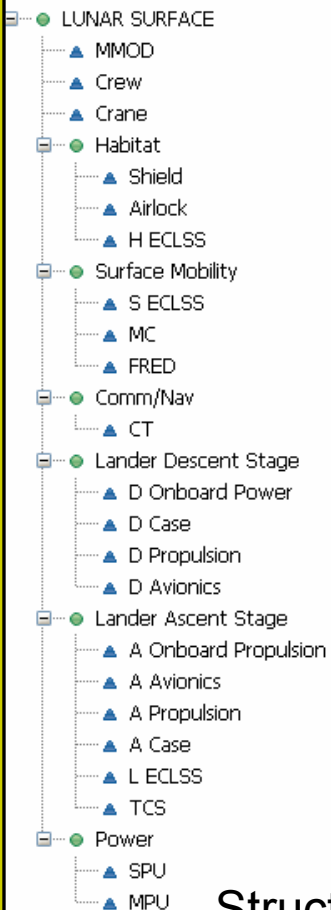
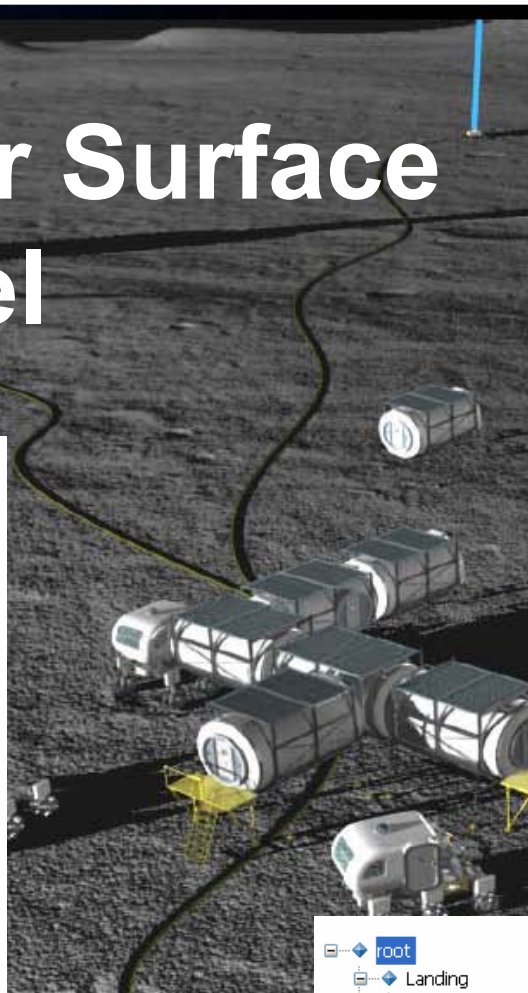


Type of Engineering Knowledge	Captured by	
	Binary planner	Multi-state planner
System elements and hierarchy	Structure Tree	Structure Tree
Elements' states and operational modes	Assumed binary (work or fail)	Structure Tree
Functionalities/ Activities/Events provided/Acted upon by elements	Functionalities 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

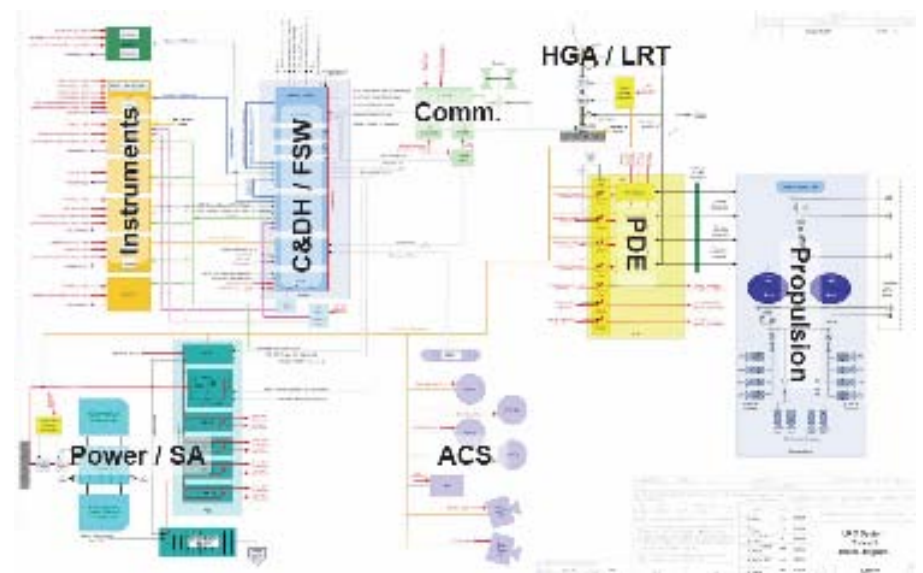
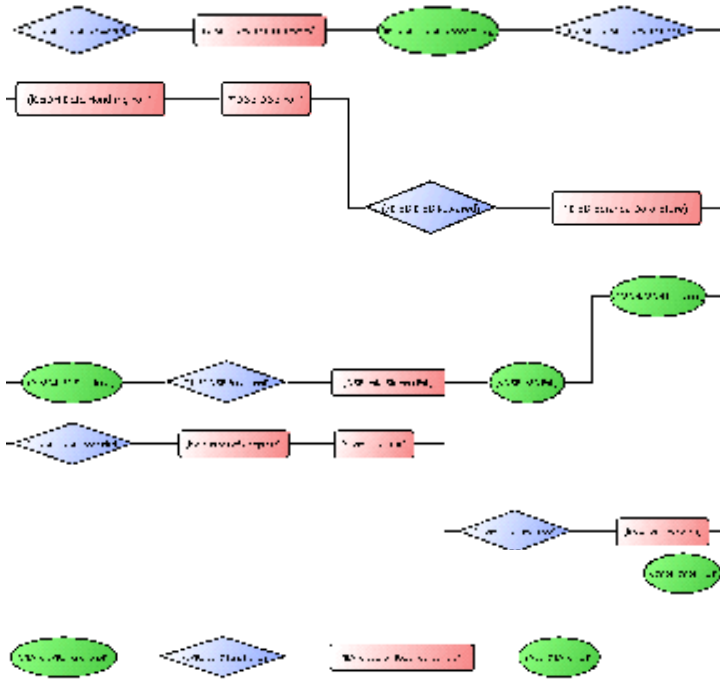
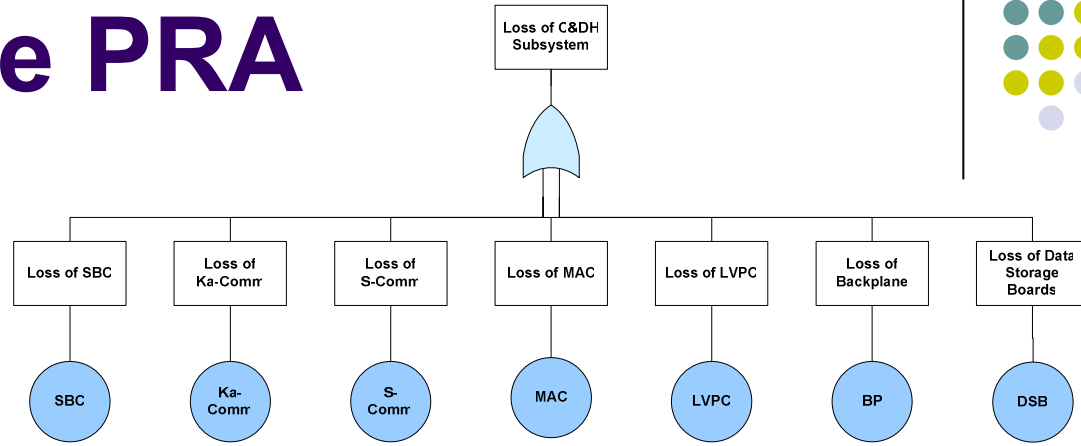
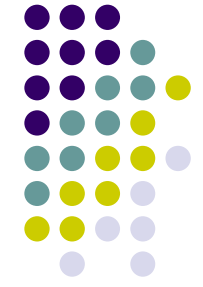
Reference Lunar Sortie Mission



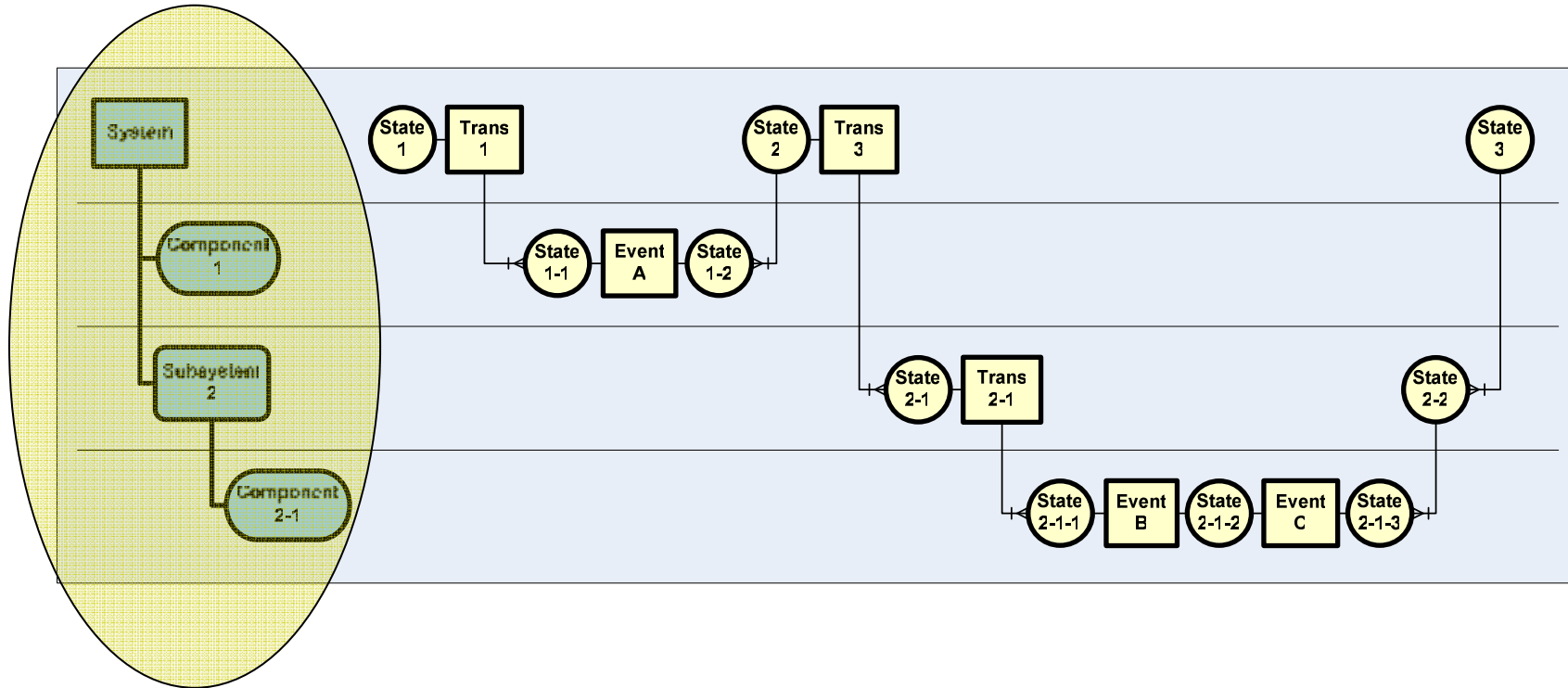
Lunar Surface model



LRO Satellite PRA



Example of a Generated Plan (Event Sequence Diagram)



Plan Updating



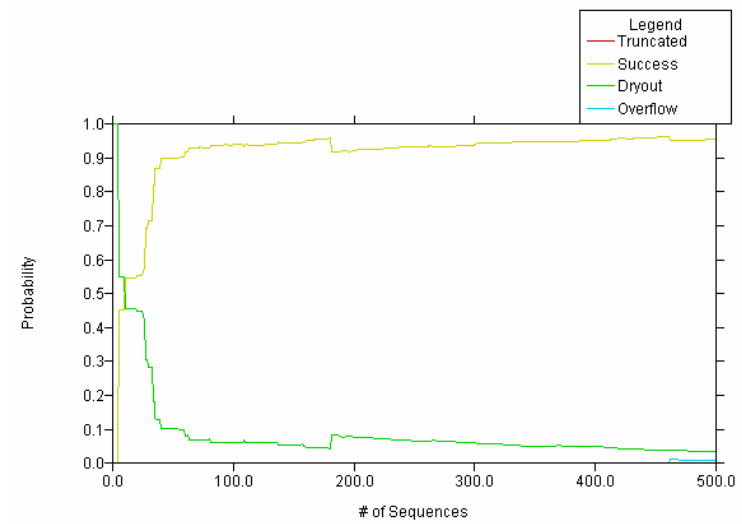
When a predefined number of simulation-runs are completed

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



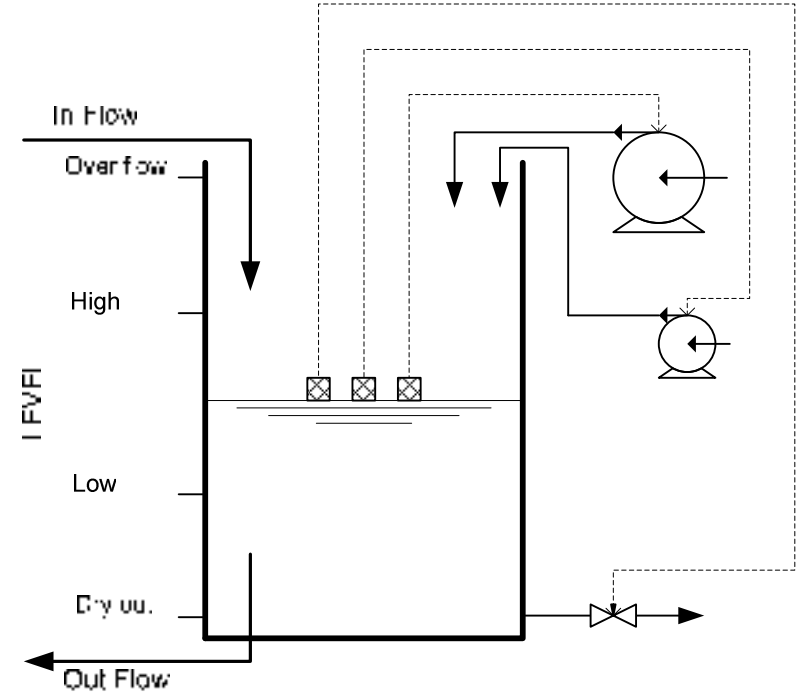
```

sim_planning.txt - Notepad
...
< Param_BallValve_1:ValvePosition: Param_PumpOff_1:ValvePosition: Param_PumpOn_1:ValvePosition:Off Pump_1
< Param_BallValve_2:ValvePosition: Param_PumpOff_2:ValvePosition: Param_PumpOn_2:ValvePosition:Off Pump_2
< Param_BallValve_3:ValvePosition: Param_PumpOff_3:ValvePosition: Param_PumpOn_3:ValvePosition:Off Pump_3
< Param_BallValve_4:ValvePosition: Param_PumpOff_4:ValvePosition: Param_PumpOn_4:ValvePosition:Off Pump_4
< Param_BallValve_5:ValvePosition: Param_PumpOff_5:ValvePosition: Param_PumpOn_5:ValvePosition:Off Pump_5
< Param_BallValve_6:ValvePosition: Param_PumpOff_6:ValvePosition: Param_PumpOn_6:ValvePosition:Off Pump_6
< Param_BallValve_7:ValvePosition: Param_PumpOff_7:ValvePosition: Param_PumpOn_7:ValvePosition:Off Pump_7
< Param_BallValve_8:ValvePosition: Param_PumpOff_8:ValvePosition: Param_PumpOn_8:ValvePosition:Off Pump_8
< Param_BallValve_9:ValvePosition: Param_PumpOff_9:ValvePosition: Param_PumpOn_9:ValvePosition:Off Pump_9
< Param_BallValve_10:ValvePosition: Param_PumpOff_10:ValvePosition: Param_PumpOn_10:ValvePosition:Off Pump_10
< Param_BallValve_11:ValvePosition: Param_PumpOff_11:ValvePosition: Param_PumpOn_11:ValvePosition:Off Pump_11
< Param_BallValve_12:ValvePosition: Param_PumpOff_12:ValvePosition: Param_PumpOn_12:ValvePosition:Off Pump_12
< Param_BallValve_13:ValvePosition: Param_PumpOff_13:ValvePosition: Param_PumpOn_13:ValvePosition:Off Pump_13
< Param_BallValve_14:ValvePosition: Param_PumpOff_14:ValvePosition: Param_PumpOn_14:ValvePosition:Off Pump_14
< Param_BallValve_15:ValvePosition: Param_PumpOff_15:ValvePosition: Param_PumpOn_15:ValvePosition:Off Pump_15
< Param_BallValve_16:ValvePosition: Param_PumpOff_16:ValvePosition: Param_PumpOn_16:ValvePosition:Off Pump_16
< Param_BallValve_17:ValvePosition: Param_PumpOff_17:ValvePosition: Param_PumpOn_17:ValvePosition:Off Pump_17
< Param_BallValve_18:ValvePosition: Param_PumpOff_18:ValvePosition: Param_PumpOn_18:ValvePosition:Off Pump_18
< Param_BallValve_19:ValvePosition: Param_PumpOff_19:ValvePosition: Param_PumpOn_19:ValvePosition:Off Pump_19
< Param_BallValve_20:ValvePosition: Param_PumpOff_20:ValvePosition: Param_PumpOn_20:ValvePosition:Off Pump_20
  
```

Scheduler GUI

Task Name	Start	End	Inter-leave
Task 1	0:00	0:00	-
Task 2	0:00	0:00	10
Task 3	0:00	0:00	10
Task 4	0:00	0:00	-

#	Sequence	Task	Start	End	Weight	# Sequences
1	0001	Task 1	0:00	0:00	1	1
2	0002	Task 2	0:00	0:00	1	2
3	0003	Task 3	0:00	0:00	1	3
4	0004	Task 1	0:00	0:00	1	4
5	0005	Task 2	0:00	0:00	1	5
6	0006	Task 3	0:00	0:00	1	6
7	0007	Task 1	0:00	0:00	1	7
8	0008	Task 2	0:00	0:00	1	8
9	0009	Task 3	0:00	0:00	1	9
10	0010	Task 1	0:00	0:00	1	10



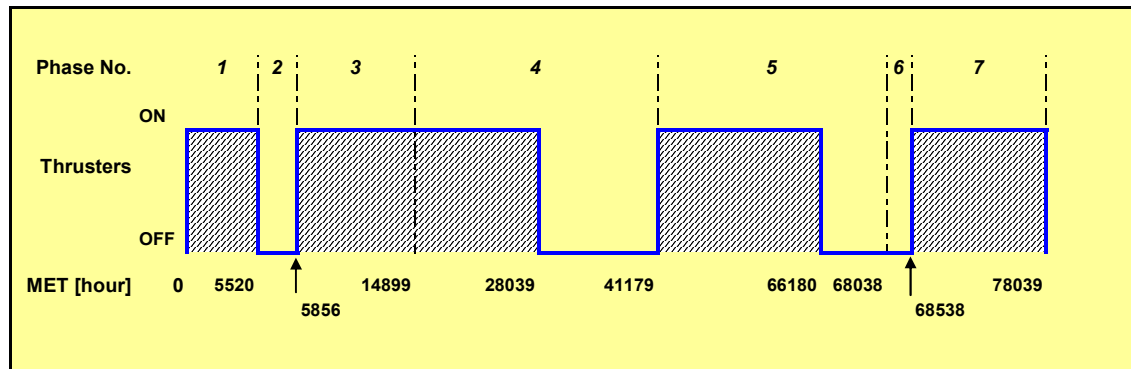
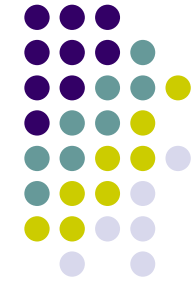
Holdup tank results



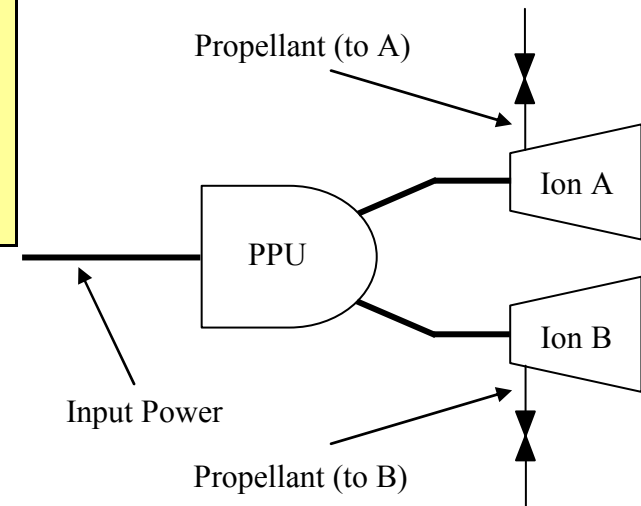
		Probability			SD	# Sequences		
		case 1	case 2	case 3		case 1	case 2	case 3
With Plan	Success	9.90E-01	9.88E-01	9.92E-01	2.00E-03	103	97	73
	Dry-out	9.73E-03	1.18E-02	7.88E-03	1.96E-03	350	353	371
	Overflow	9.02E-05	1.64E-04	1.39E-04	3.75E-05	47	50	56
Without Plan	Success	9.44E-01	9.53E-01	8.89E-01	3.46E-02	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

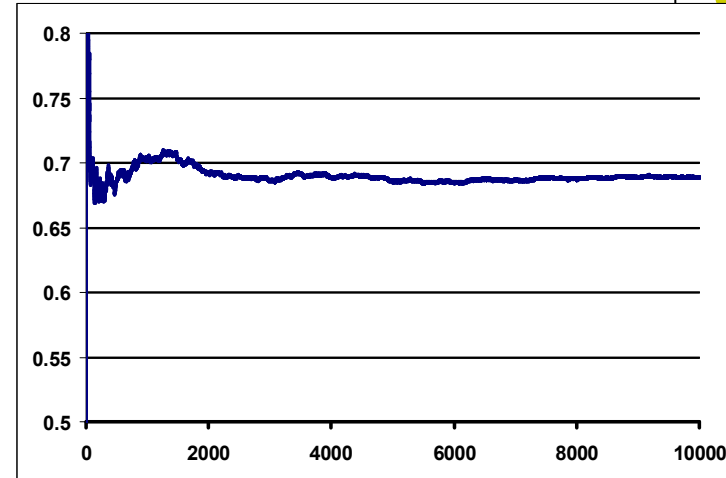
Sample Result and Comparison



SimPRA Simulation

(500 runs)

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



Monte Carlo Simulation

(10000 runs)

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]