

An Heritage Approach to Aerospace Risk Based Design: With Application

Presented at:

**SRA Workshop on Risk Analysis of Aerospace Systems II:
Mission success Starts with Safety
28-29 October 2002**

Presented by:

Joseph R. Fragola

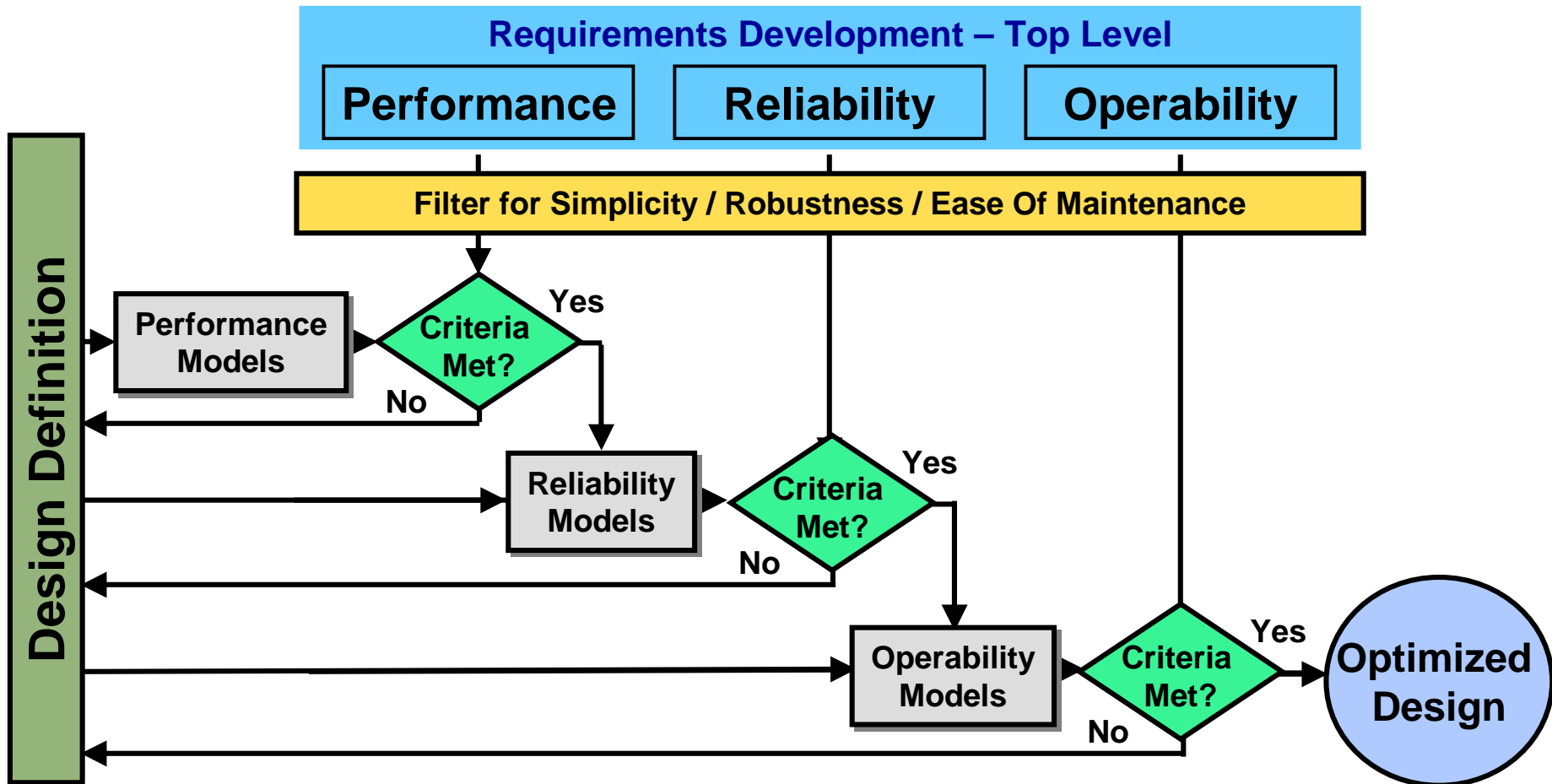
Vice President and Principal Scientist



Science Applications International Corp.

265 Sunrise Highway, Suite 22, Rockville Centre, NY 11570

Risk Based Top Down Design

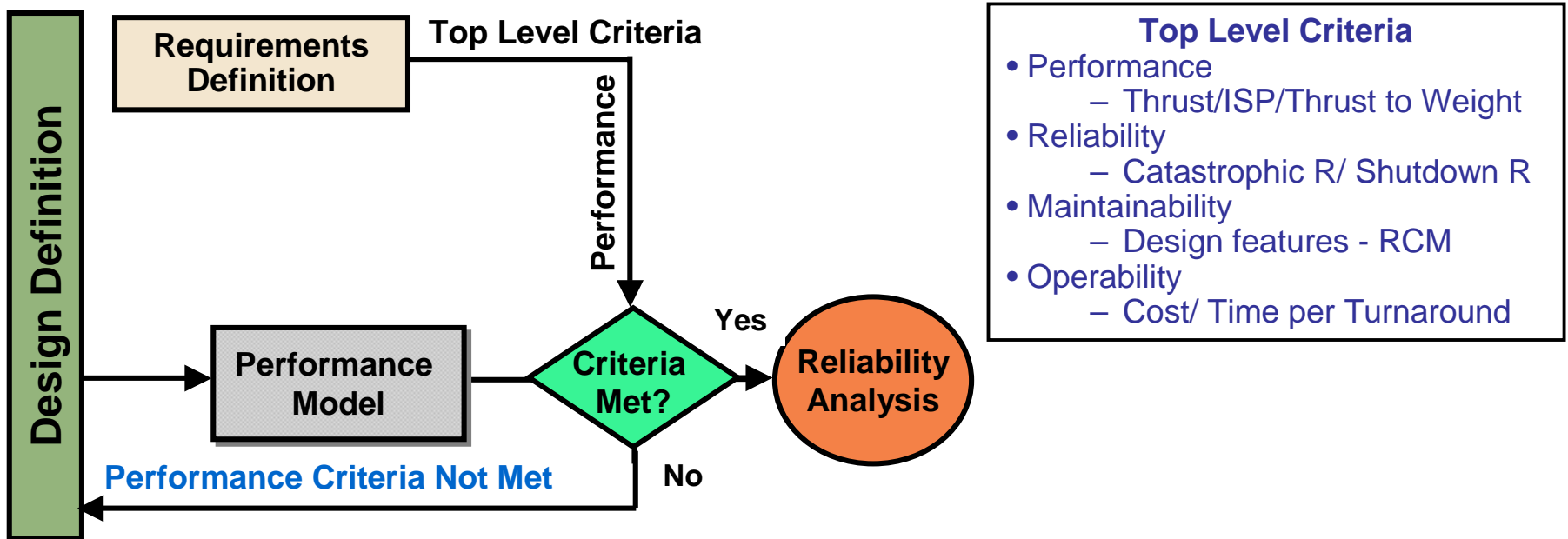


Identify the sets of design options that converge on requirements

Three Pillars of Good Design

- **Make it work**
 - Does it satisfy the requirements?
- **Make it safe**
 - Does it meet the Safety goals?
- **Make it cost effective**
 - Does it comply with budgetary constraints?

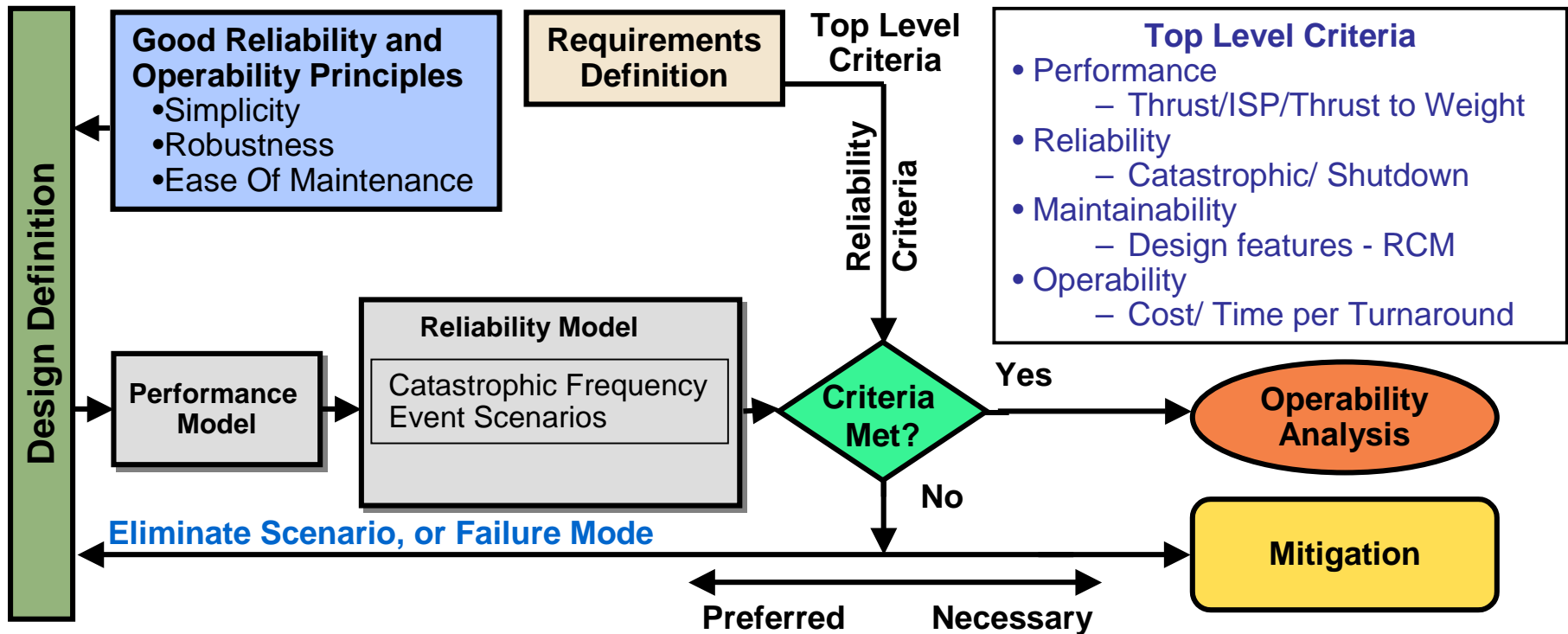
Make It Work



Performance Optimization Design Loop – Does it work?

- Inputs are the system definition
- Functionality model takes system definition and calculates performance
- If basic performance and engineering criteria are not met, iterate design
- This Performance loop is mostly complete at ConDR

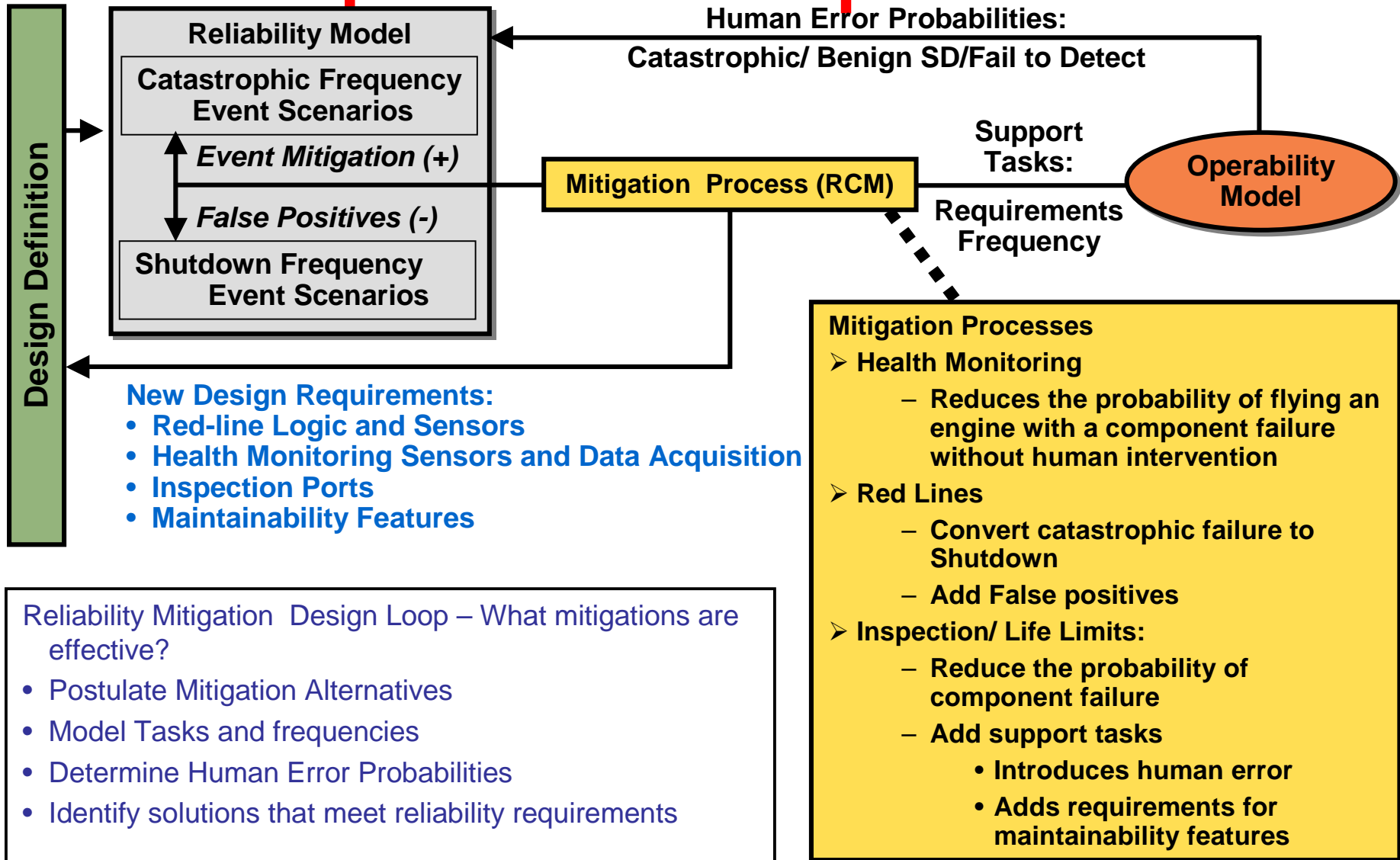
Make It Safe



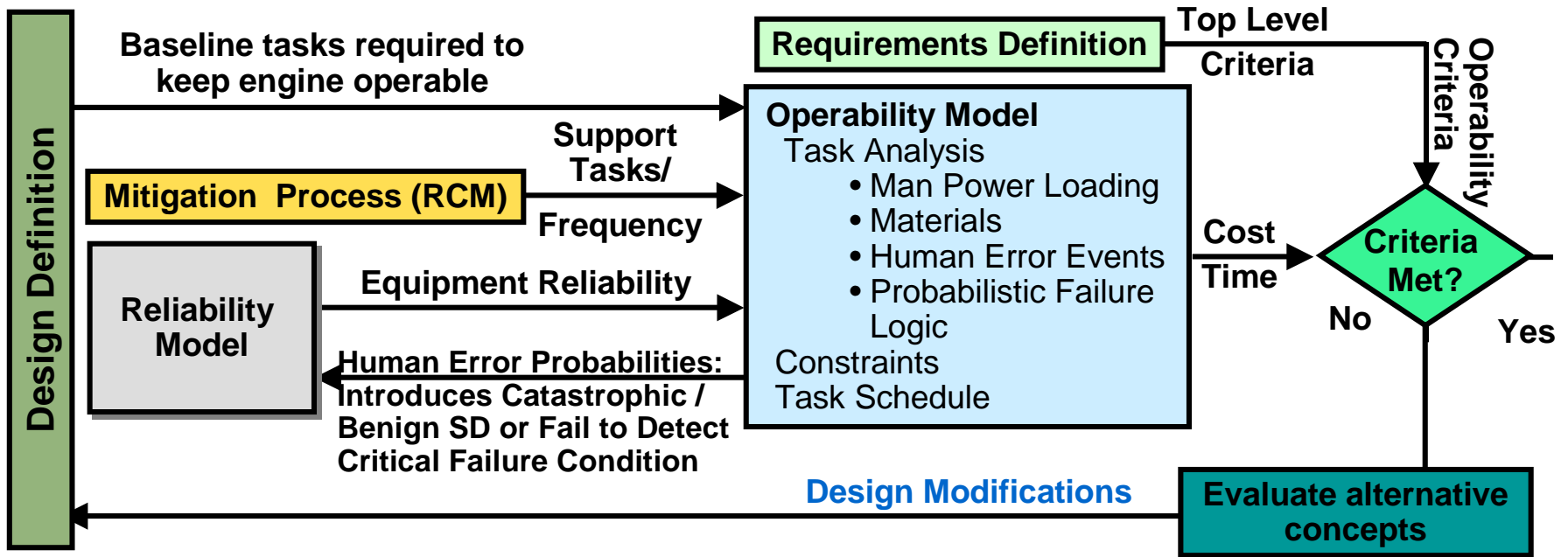
Reliability Optimization Design Loop – Is it Reliable Enough?

- Reliability model is based on heritage where possible
- Heritage is extended using probabilistic stress analysis to determine robustness
- Fault tolerance and redundancy are analyzed from system configuration
- If reliability requirements are not met, increase design margins and re-calculate performance
- If new design margins cause performance requirements to be overly compromised identify mitigation strategies

Reliability Mitigation Trade / Optimization Expansion



Make It Cost Effective



Maintainability/Supportability Optimization Design Loop

- Do support costs and schedule meet requirements? Evaluate Turn Around Time and Cost
- Identify Drivers, Optimize Process
- If Criteria not met: Identify alternative solutions that meet cost requirements
 - Modify tasks: **Streamline Operations / Reduce human error / Facilitate maintenance tasks**
 - Modify design: **Reduce maintenance requirements (robustness) / Optimize design for ease of maintenance (Simplicity) / Facilitate maintenance tasks (RCM)**

Risk Driver Identification

- In general, review WBS of each alternative
- Identify those WBS elements which are risk drivers
- Risk driver implies uncertainty in development with significant potential impact on program cost and schedule
- Historical risk drivers; propulsion, staging, multiple engine manifolding, thermal protection

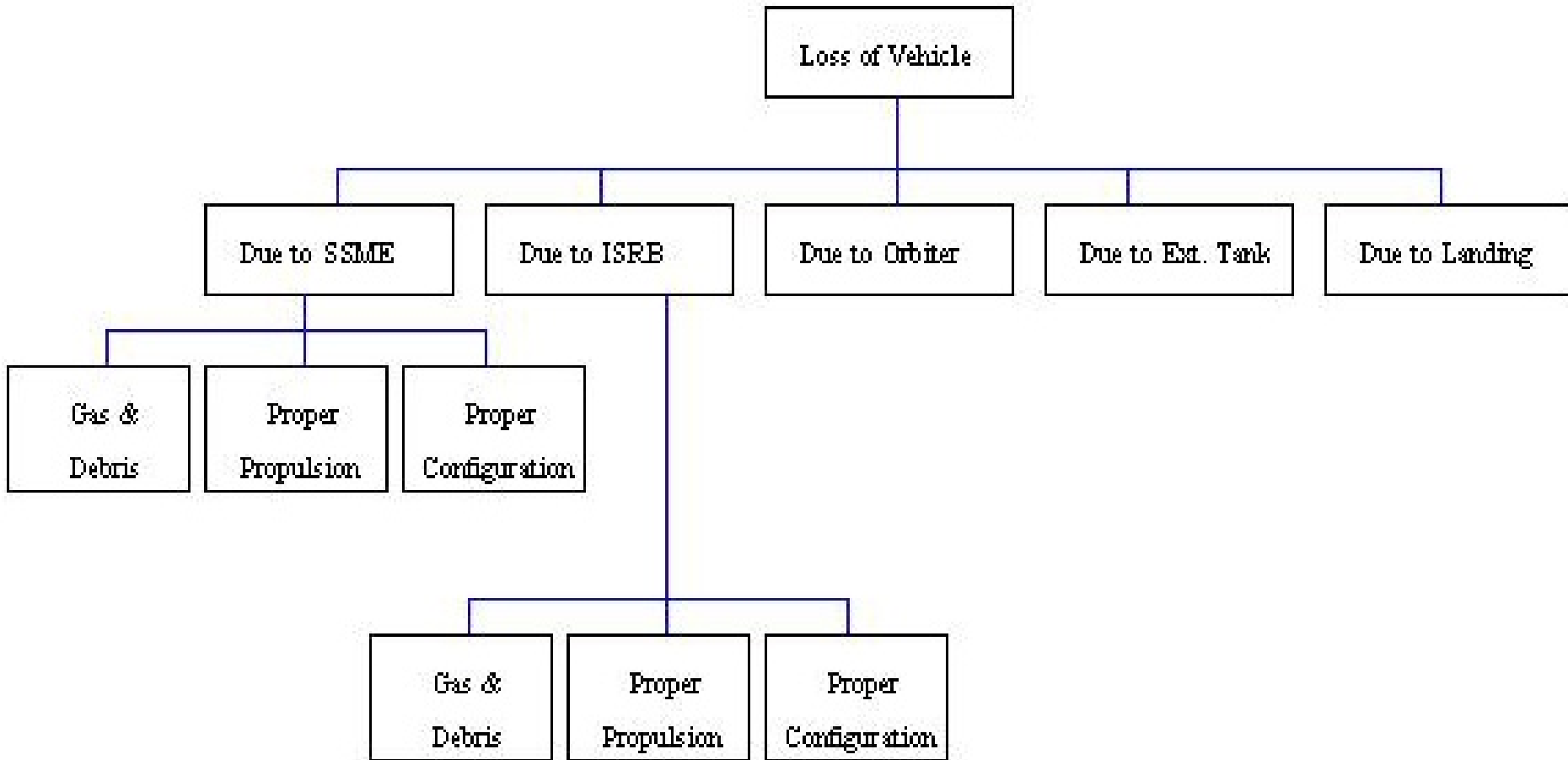
Develop Risk-focused WBS

- Trim hierarchy for low heritage risk
- Expand for high heritage risk
- WBS levels reflect risk driving elements of alternative

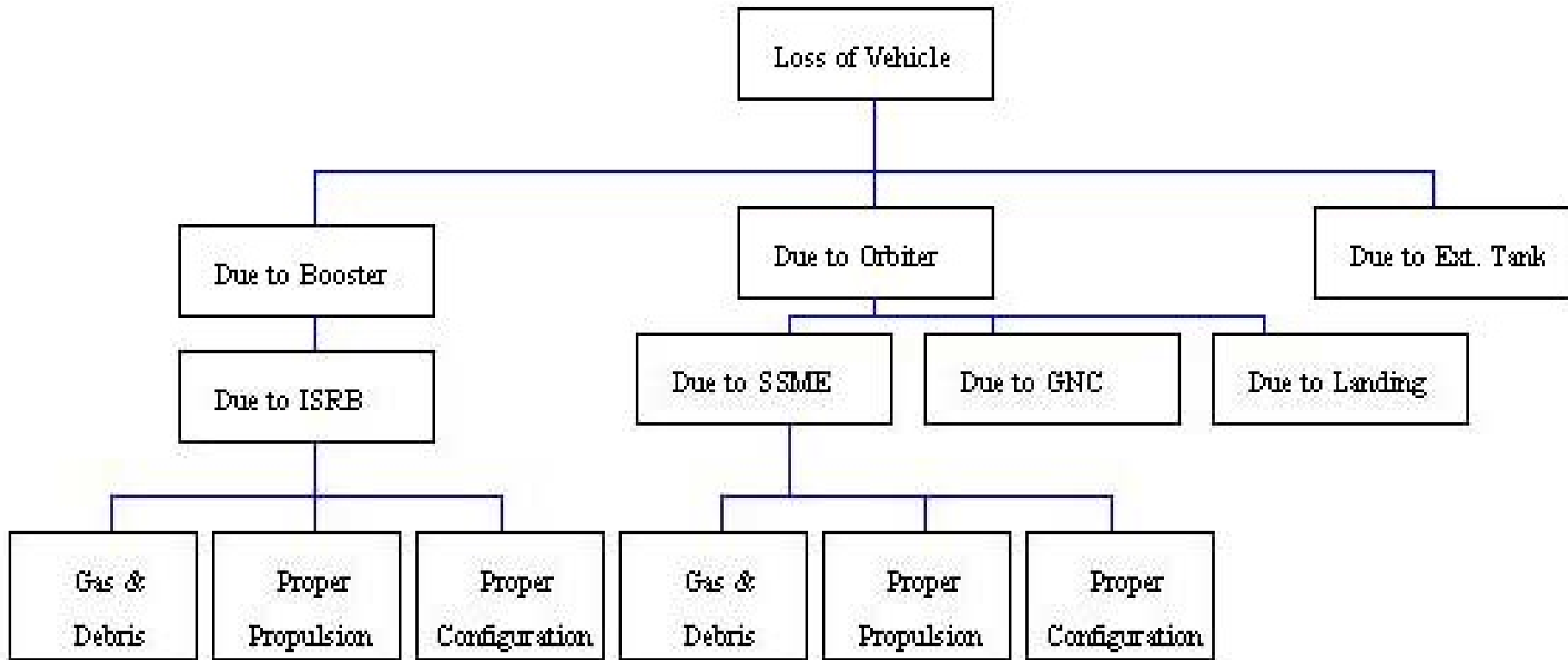
Development of Surrogate(s)

- Review heritage for potential surrogates
- Develop component functional representation of WBS for surrogate
- Develop or modify surrogate risk model into component functional (“lego block”) form
- Map surrogate to new alternative
- Modify risk models as appropriate
- Estimate risk from surrogate as modified

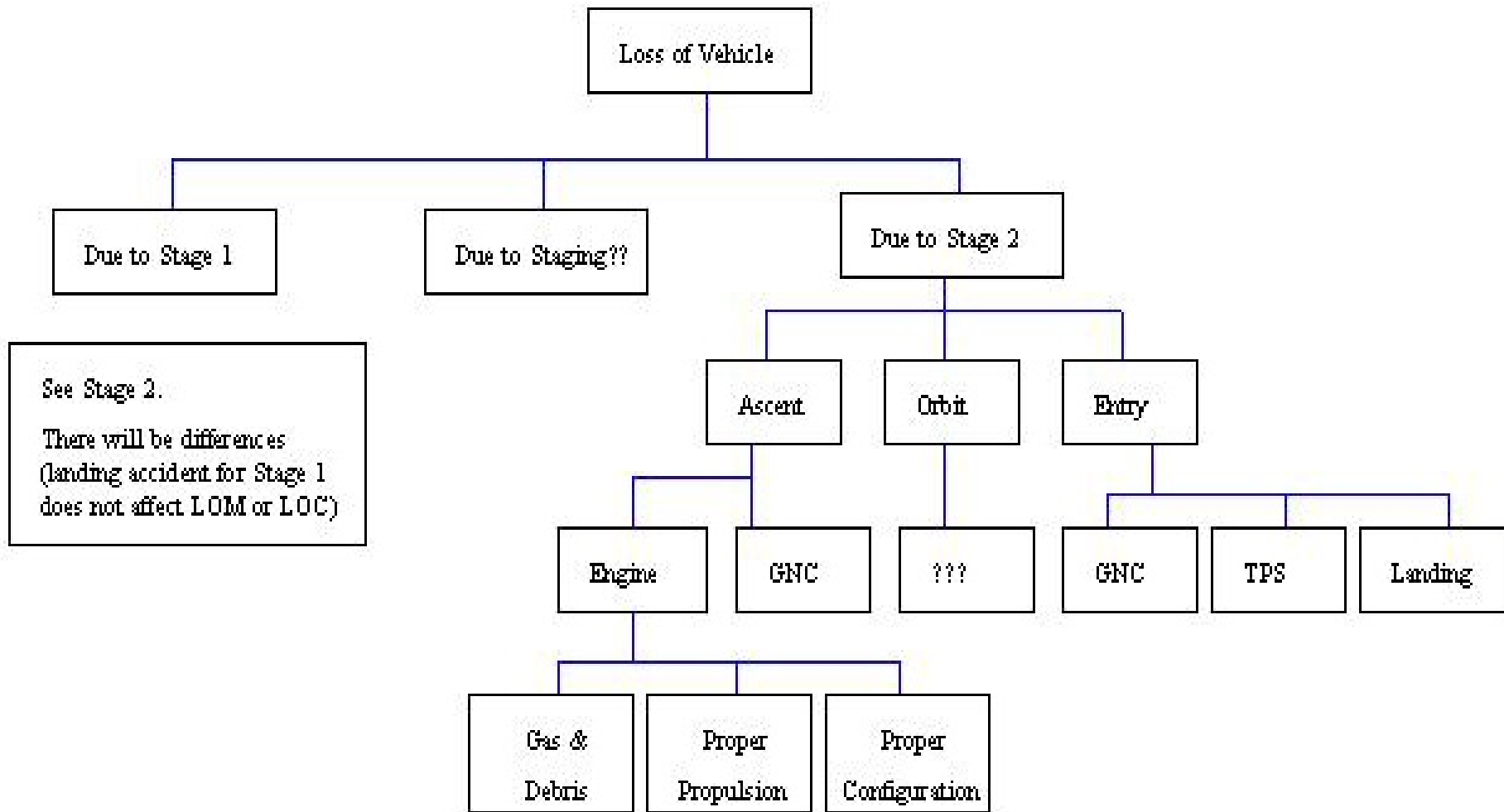
Top Level of Shuttle PRA 1995 Study



Shuttle PRA Restructured WBS Oriented



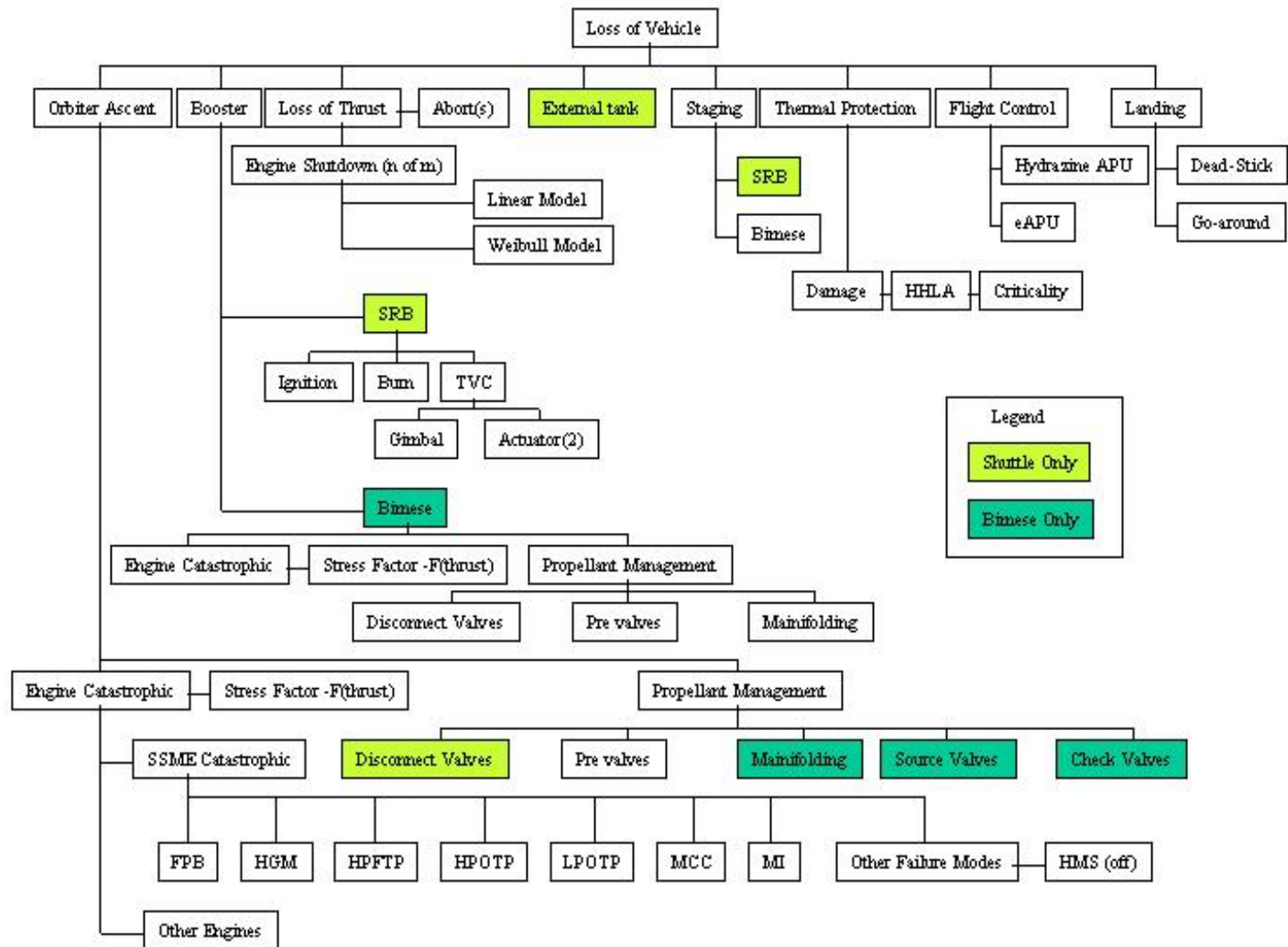
Shuttle PRA Restructured for Multistage Launcher



PRA Structure Mapping

- Choose top event
- Identify overlap events
- Identify non-applicable events
- Identify alternate unique events

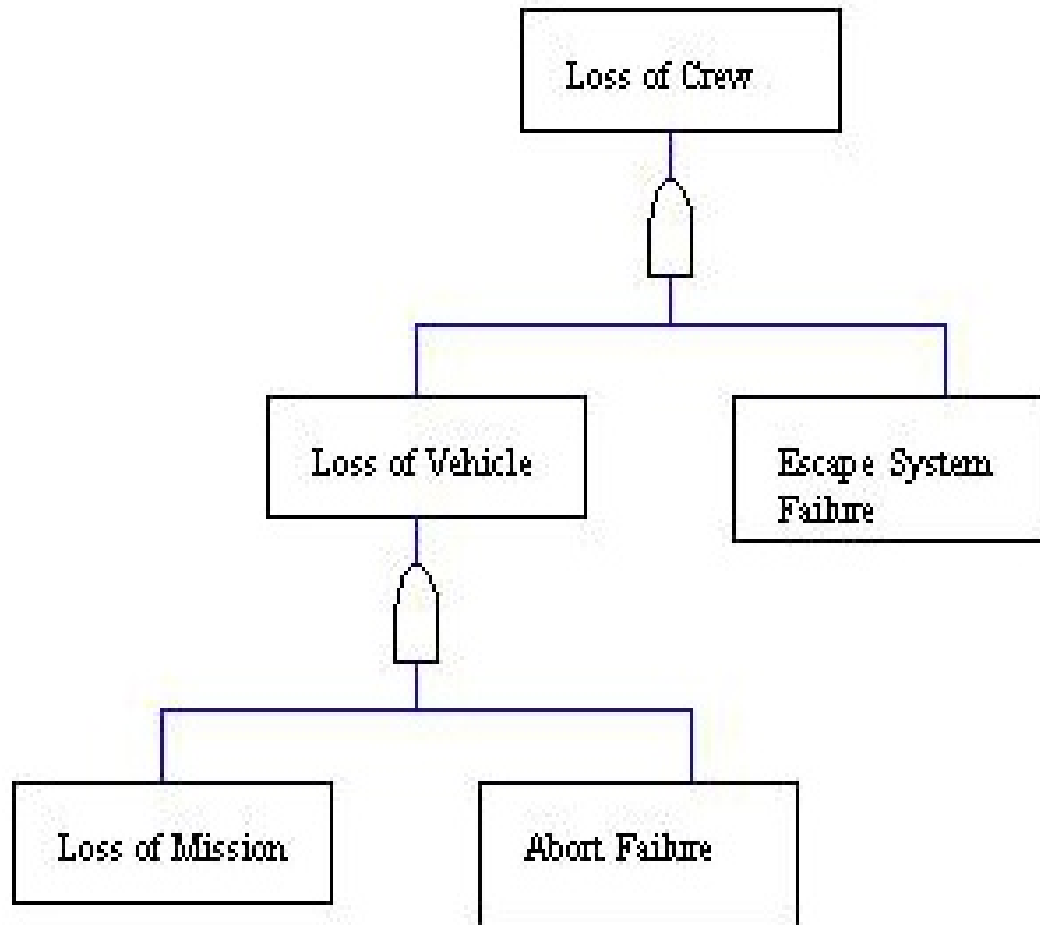
RLV Loss of Vehicle (LOV) Model (Bimese Example)



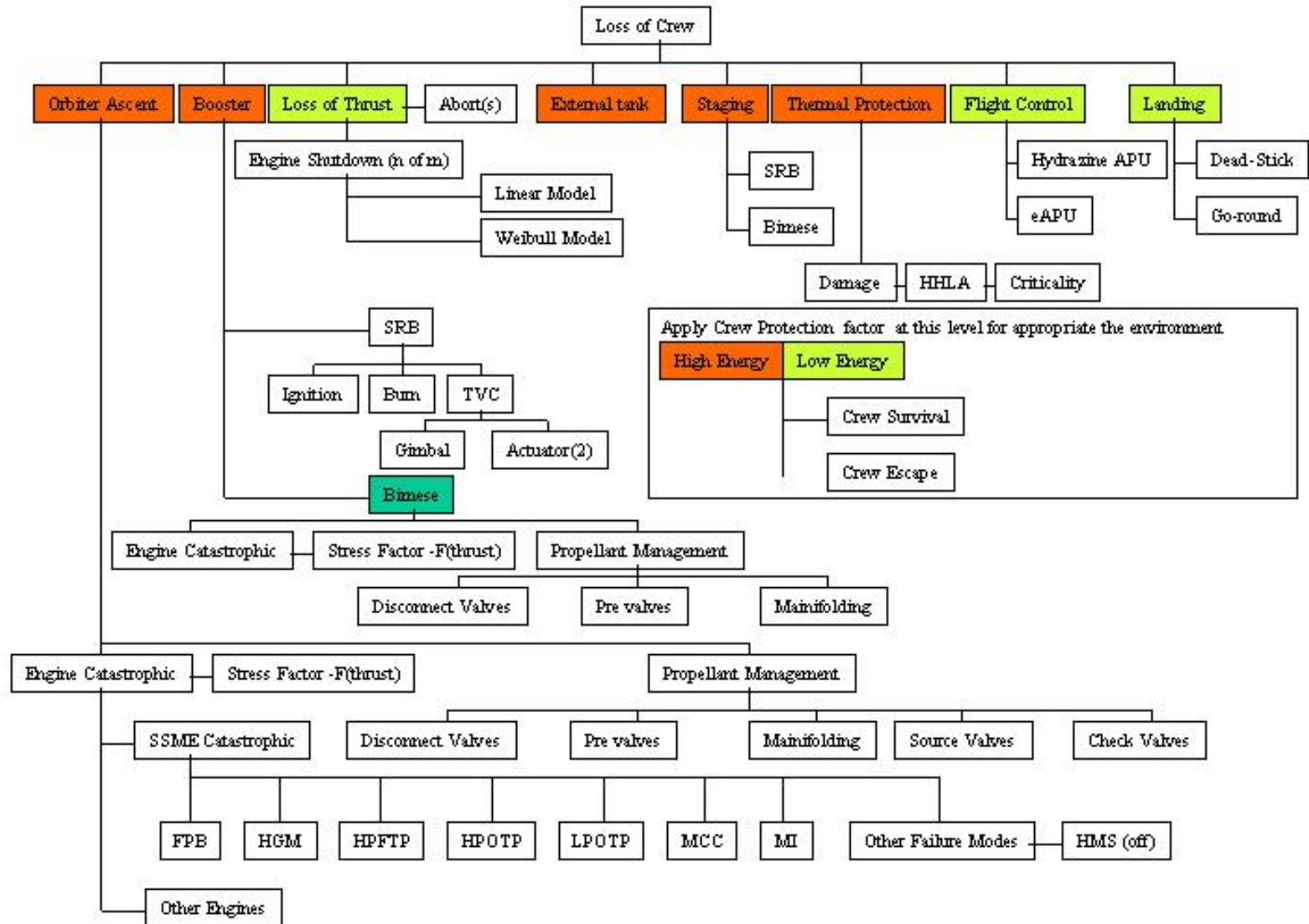
Quantification via Surrogate

- Add additional surrogates as appropriate
- Develop models for remaining unique elements
- Integrate models
- Quantify risk with integrated models

Shuttle PRA Expanded to Include Crew Escape

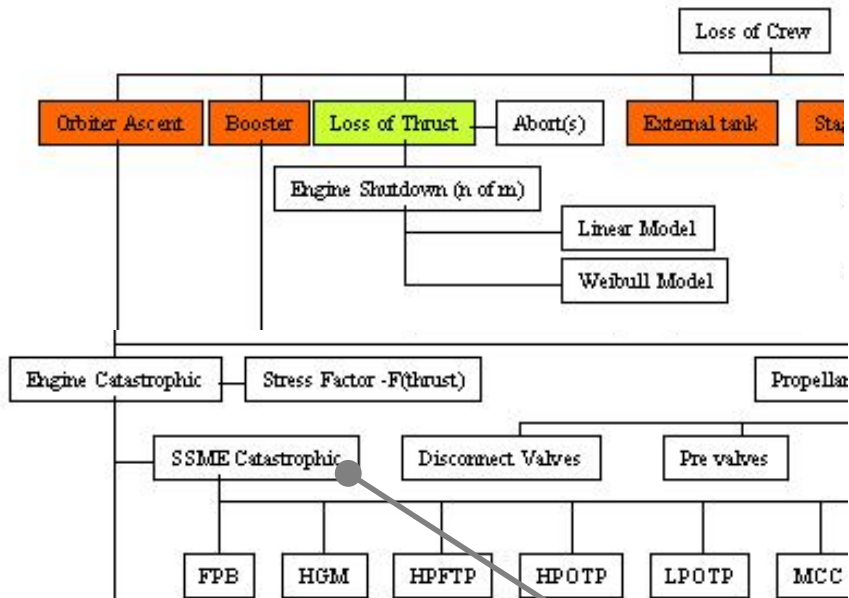


RLV Loss of Crew (LOC) Model (Bimese Model)



STS PRA Generalization

Functional “Lego” Block Definition



Model Name

- ENG_CAT_SSME_97
- ENG_CAT
- ENG_CAT_ADJ
- ENG_CAT_COBRA
- ENG_CAT_SSME_95
- ENG_CAT_SSME_97**
- ENG_CAT_SSME_COBL

ENG_CAT_ADJ	1.97E-03
ENG_CAT_COBRA	1.98E-03
ENG_CAT_SSME_95	1.97E-03
ENG_CAT_SSME_97	1.99E-03
ENG_CAT_COBL	1.96E-03

Risk Model – Baseline Shuttle Results

Risk Model					
LOV Model Element	Model	Number	LOV	Energy	LOC
Oribiter Engine Catastrophic Failure	ENG_CAT_SSME_97	3	1.97E-03	HE	1.97E-03
Oribiter Propellant Management Check Valve	PM_CHK	0	0.00E+00	HE	0.00E+00
Oribiter Propellant Management Disconnect Valve	PM_DISC_FC	2	1.30E-06	HE	1.30E-06
Oribiter Propellant Management Feed Valve	PM_FEED	0	0.00E+00	HE	0.00E+00
Oribiter Propellant Management Manifold	PM_MAN	0	0.00E+00	HE	0.00E+00
Oribiter Propellant Management Pre Valve	PM_PRE_FC	6	1.75E-05	HE	1.75E-05
Orbiter_Ascent			1.98E-03	HE	1.98E-03
SRB Actuator	SRB_ACT	4	4.13E-05	HE	4.13E-05
SRB Burn	SRB_BRN	2	5.28E-04	HE	5.28E-04
SRB Gimbal	SRB_GIM	2	1.48E-05	HE	1.48E-05
SRB Ignition	SRB_IGN	2	4.80E-04	HE	4.80E-04
Booster Engine Catastrophic Failure	ENG_CAT_SSME_97	0	0.00E+00	HE	0.00E+00
Booster Propellant Management Disconnect Valve	PM_DISC_FC	0	0.00E+00	HE	0.00E+00
Booster Propellant Management Manifold	PM_MAN	0	0.00E+00	HE	0.00E+00
Booster Propellant Management Pre Valve	PM_PRE_FC	0	0.00E+00	HE	0.00E+00
Booster			1.02E-03	HE	1.02E-03
Constant Shutdown Rate	Single_Engine		0.00E+00		
Constant Shutdown Rate	Double_Engine		0.00E+00		
Constant Shutdown Rate	Triple_Engine		0.00E+00		
Weibull Shutdown	Single_Engine		0.0E+00		
Weibull Shutdown	Double_Engine		5.7E-03		
Weibull Shutdown	Triple_Engine		4.5E-03		
Binomial Failure Model	Single_Engine		0.00E+00		
Binomial Failure Model	Double_Engine		9.71E-05		
Binomial Failure Model	Triple_Engine		9.09E-08		
Loss_of_Thrust			9.71E-05	LE	9.71E-05
External_Tank	ET	1	1.91E-04	HE	1.91E-04
Staging	Stage_SRB	2	1.49E-04	HE	1.49E-04
Thermal_Protection	TPS_SH_NOM		5.00E-04	HE	5.00E-04
Flight_Control	FC_HYD		8.10E-04	LE	8.10E-04
Landing	LND_DS		4.11E-04	LE	4.11E-04
Total			5.17E-03		5.17E-03

Input Table

The screenshot shows a Microsoft Excel spreadsheet titled "Framework for Application 12-18-blake". The active sheet is "ENG_CAT_SSME_97". The spreadsheet contains an input table with the following structure:

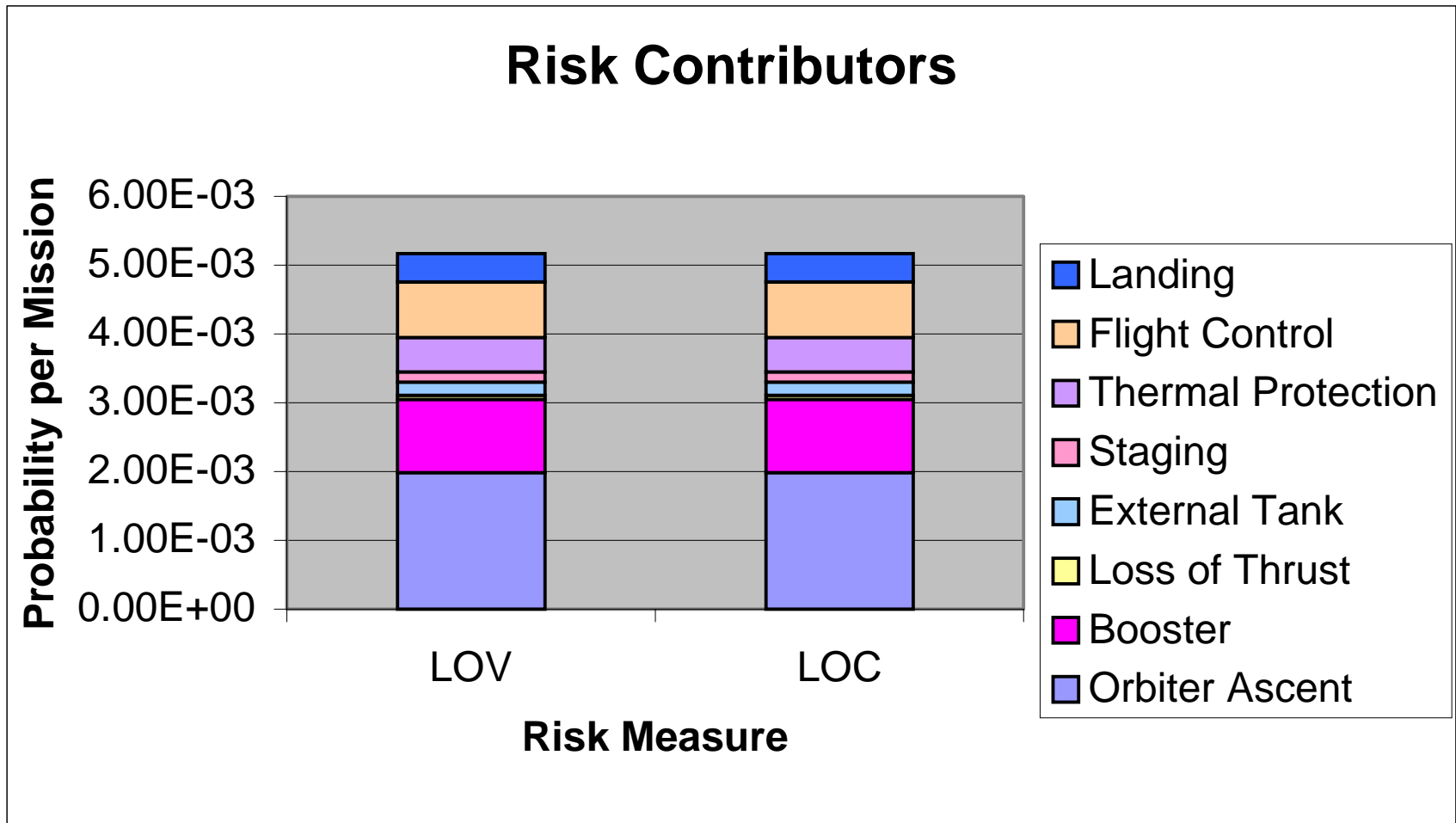
Input Variables		Mission Related		Vehicle Configuration		Value	
Orbiter_ET	226	HHLA	624	Landing			0.5
Booster_ET	126	FCF	0.69	Crew_Protection			None
Hold_Down_Time	0	Power_Level	N/A	APU			Electric
Single_Engine_Out_Time				Number_of_Orbiter_Engines			10
Double_Engine_Out_Time				Number_of_Booster_Engines			10
Triple_Engine_Out_Time				Vehicle_Type			Bimese
				TPS_Toughness			0.5
				SRB_Burn_RR_Factor			1
Alternative Engine Models		Model Name		TRL Model Inputs			
Engine_Model		ENG_CAT_SSME_97		Deployment_Date			5
Shutdown_Model		ENG_CAT		SSME_Adjust_TRL			10
Engine_SD_Rate		ENG_CAT_ADJ					
		ENG_CAT_COBRA					
		ENG_CAT_SSME_95					
		ENG_CAT_SSME_97					
		ENG_CAT_SSME_COBL					

Callouts in the image point to specific features:

- Parameters From Mission Model:** Points to the "Mission Related" columns (HHLA, FCF, Power_Level).
- Multiple Reliability Models:** Points to the "Alternative Engine Models" section, specifically the list of model names.
- Pull-down Boxes:** Points to the "Model Name" column, which is currently displaying a list of engine model options.

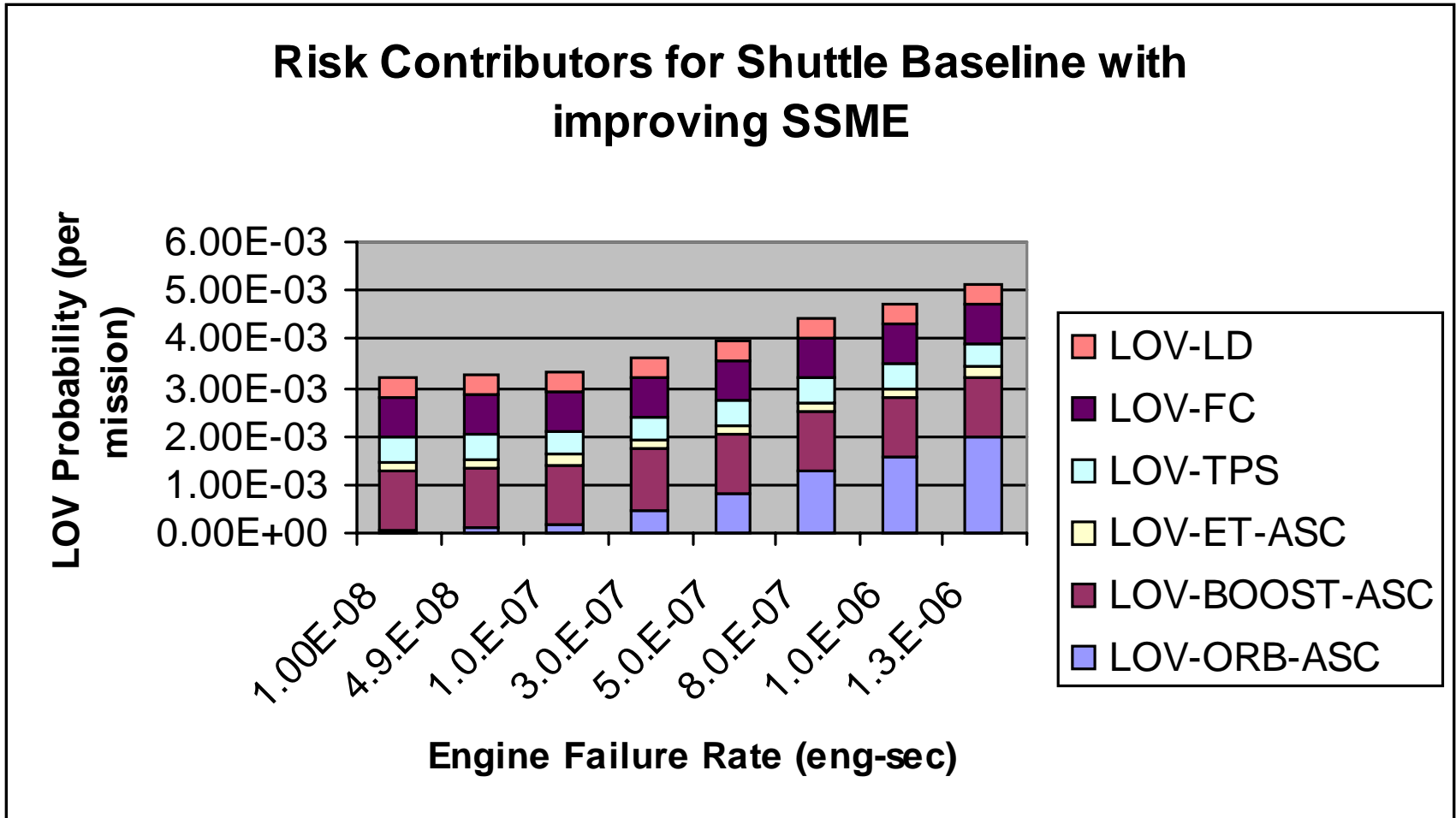
Shuttle Risk Contributors

LOV/LOC are equivalent since the Shuttle has no crew protection



Potential Impact of Candidate Technologies

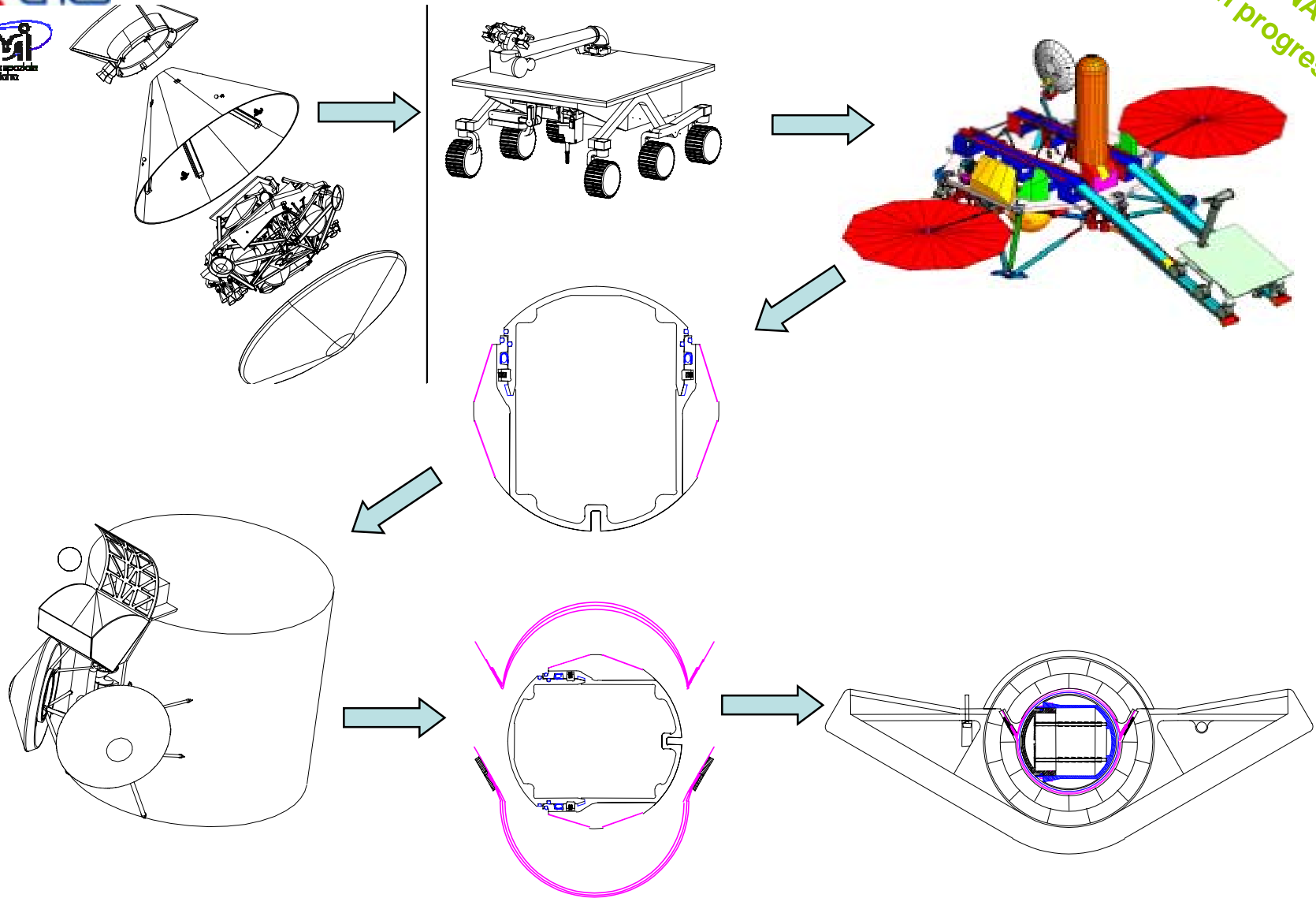
Continued component reliability improvements become less important





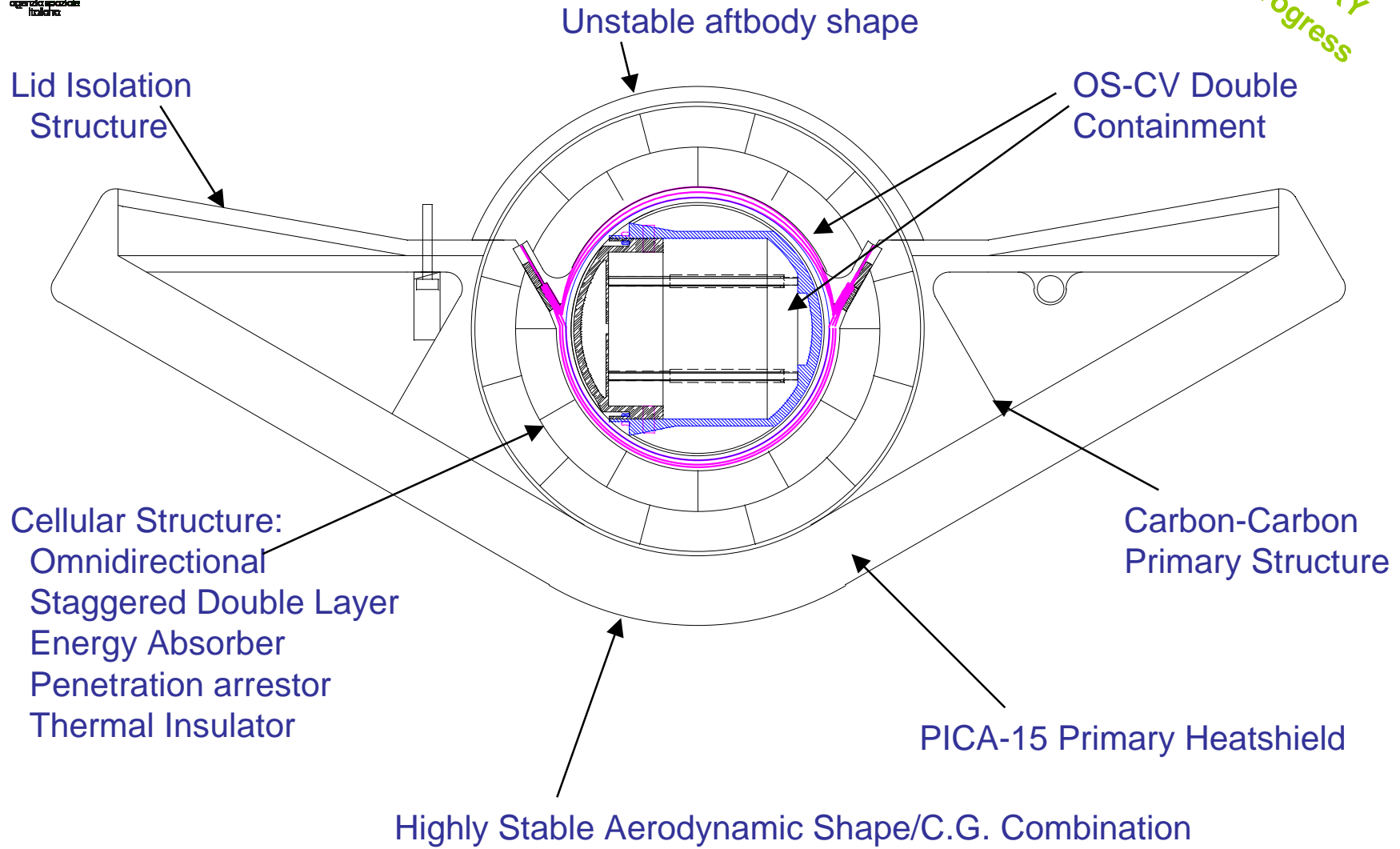
Mars Sample Return

PRELIMINARY
work in progress

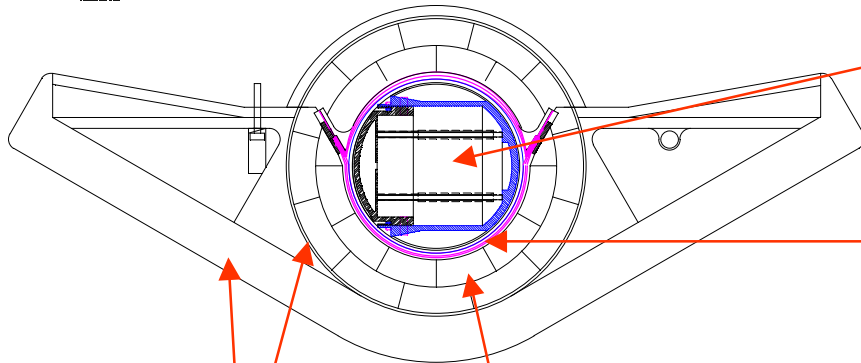


Earth Entry Vehicle

PRELIMINARY
work in progress



Assured Containment Packing Design



1: Primary Container

Sample Canister is a high strength non-permeable impact tolerant structure

Designed to survive worst case design loads.

2: Secondary Container

Containment Vessel is a high strength non-permeable impact tolerant structure.

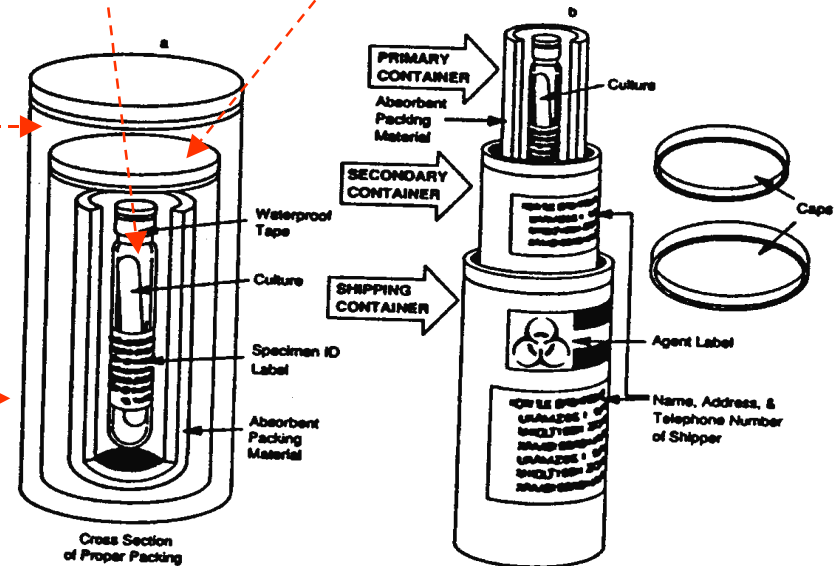
Designed to survive beyond worst case design loads 1.4 FS.

"Packing Foam"

Energy Absorption material provides G load limitation (6000 G's) for impact on rigid surface. Langley's cellular construction will also provide protection from direct rock strike.

3: Tertiary Outer Shipping Container

Impact Sphere structure provides structural integrity to prevent release of OS/CV assembly during worst case primary impact.

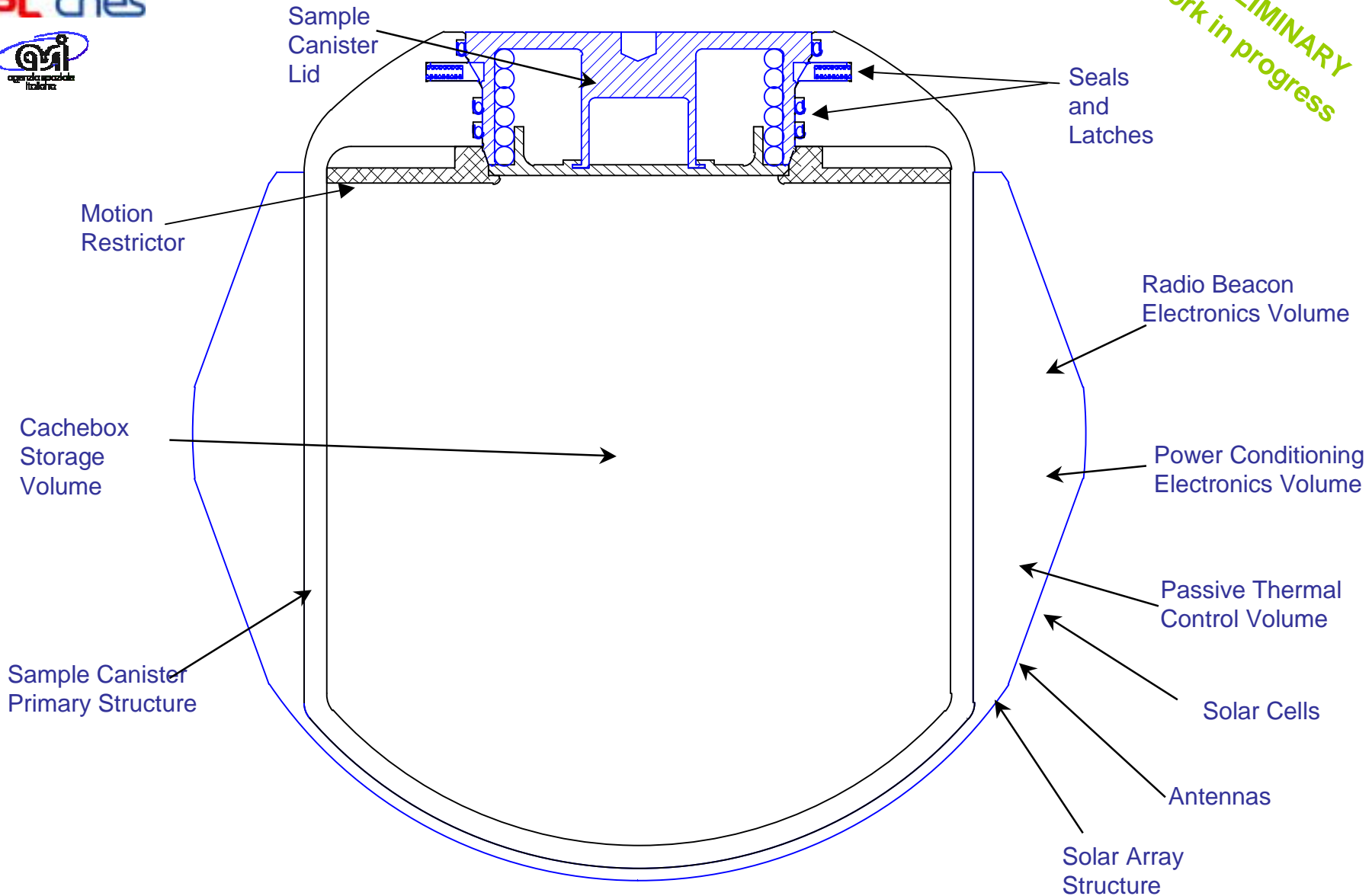


PRELIMINARY
work in progress

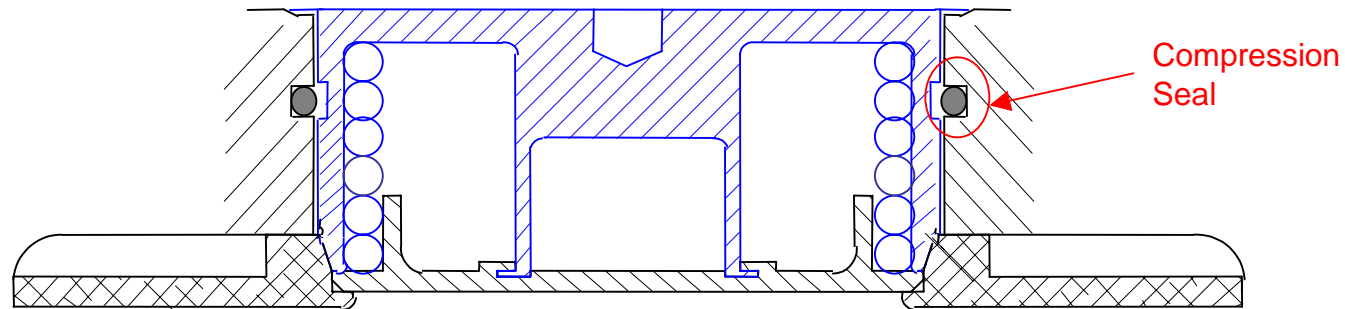


OS Configuration

PRELIMINARY
work in progress

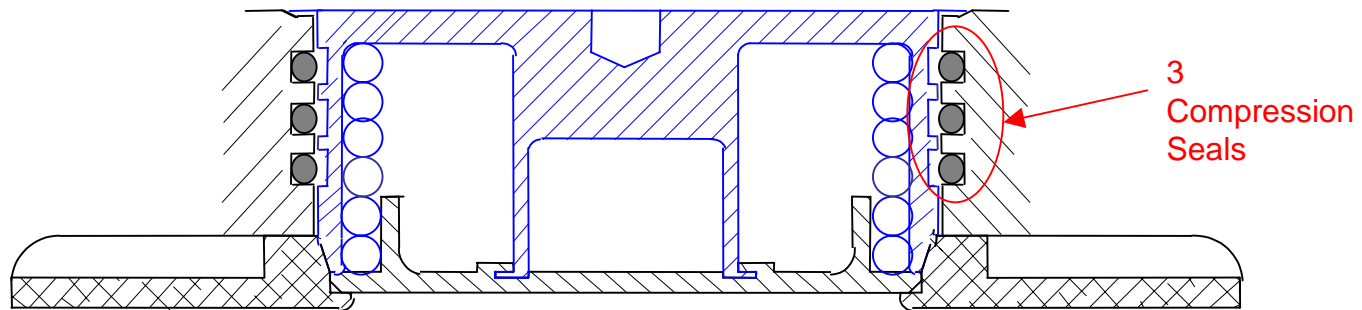


Conventional Functional Design



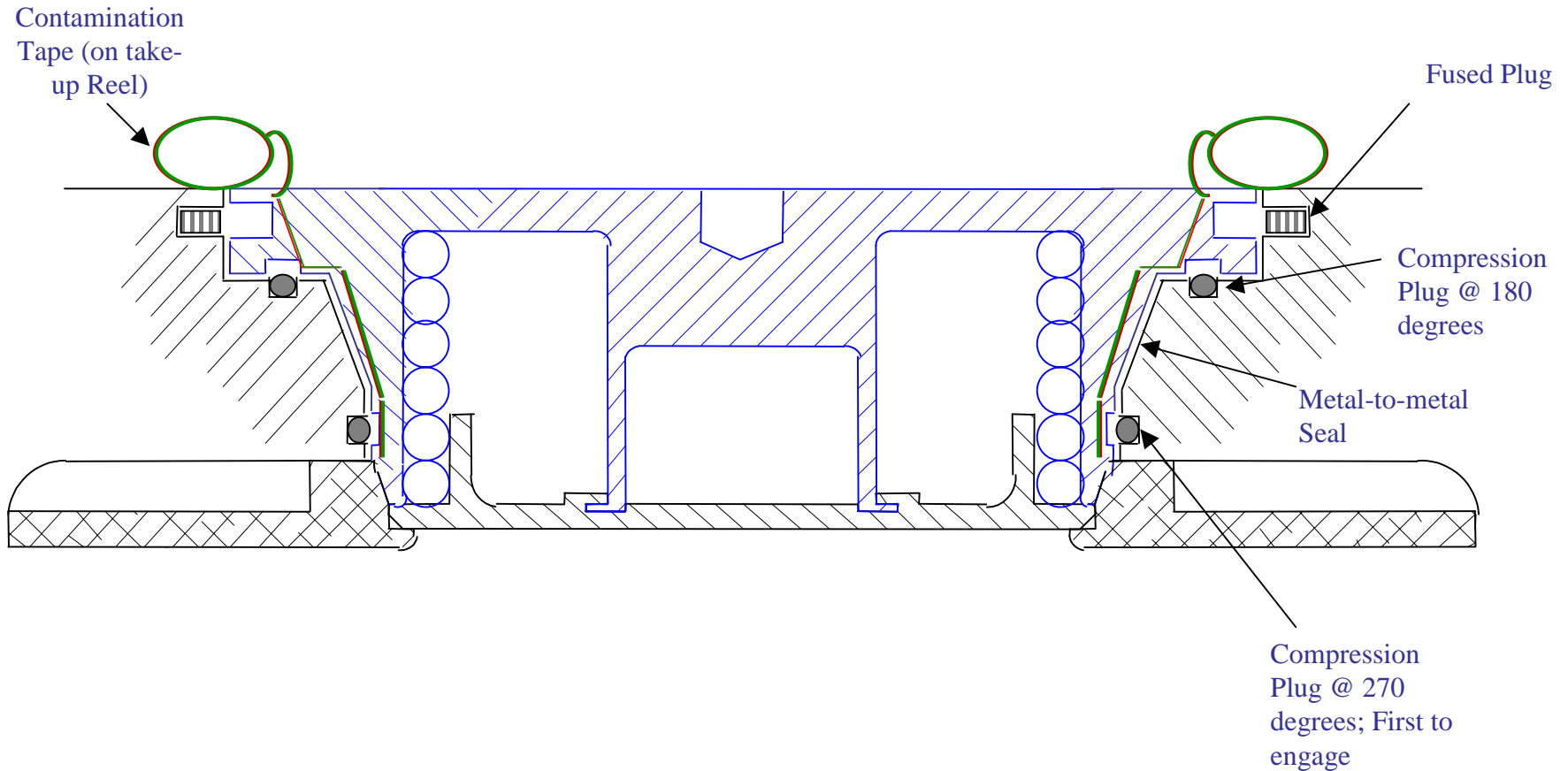
- One seal on each side suffices to perform the sealing function
- However to meet risk requirements Seal must prevent contamination release at better than $1E-6$

Risk-Based Design for Independent Failures

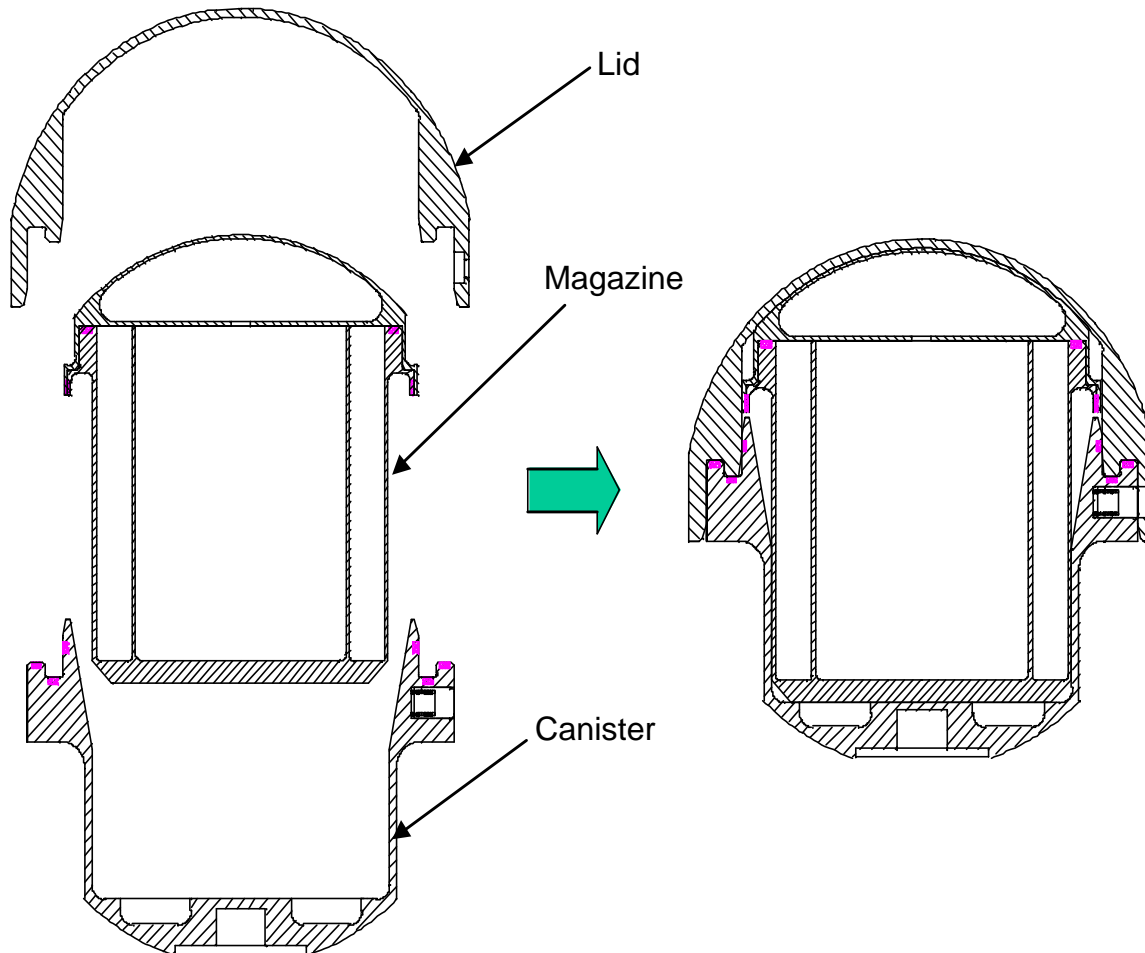


- Three seals, rather than one, satisfies both functional and independent failure risk requirements
- Here redundancy provides protection against independent seal failures

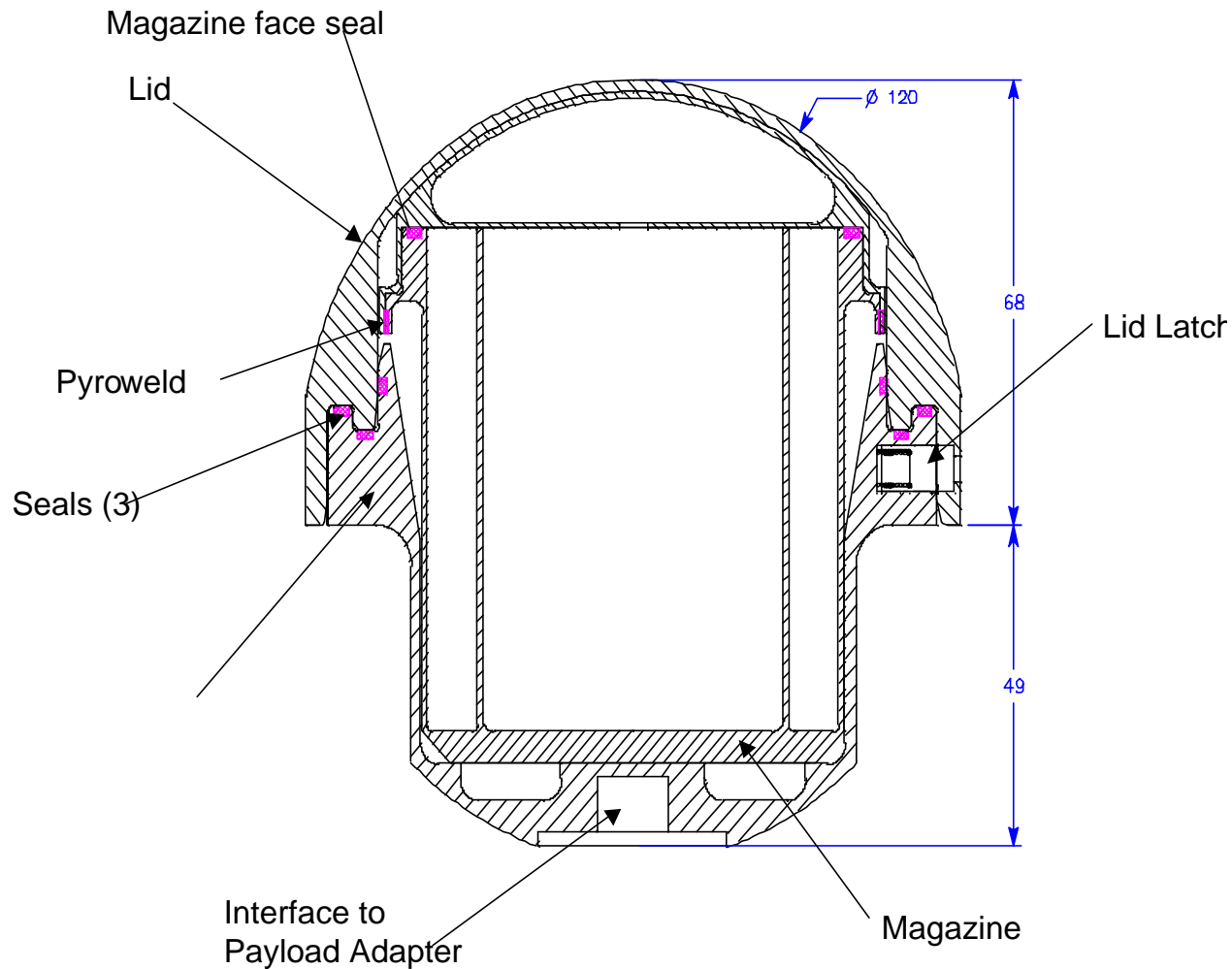
Risk-Based Design to address Contamination and CCF



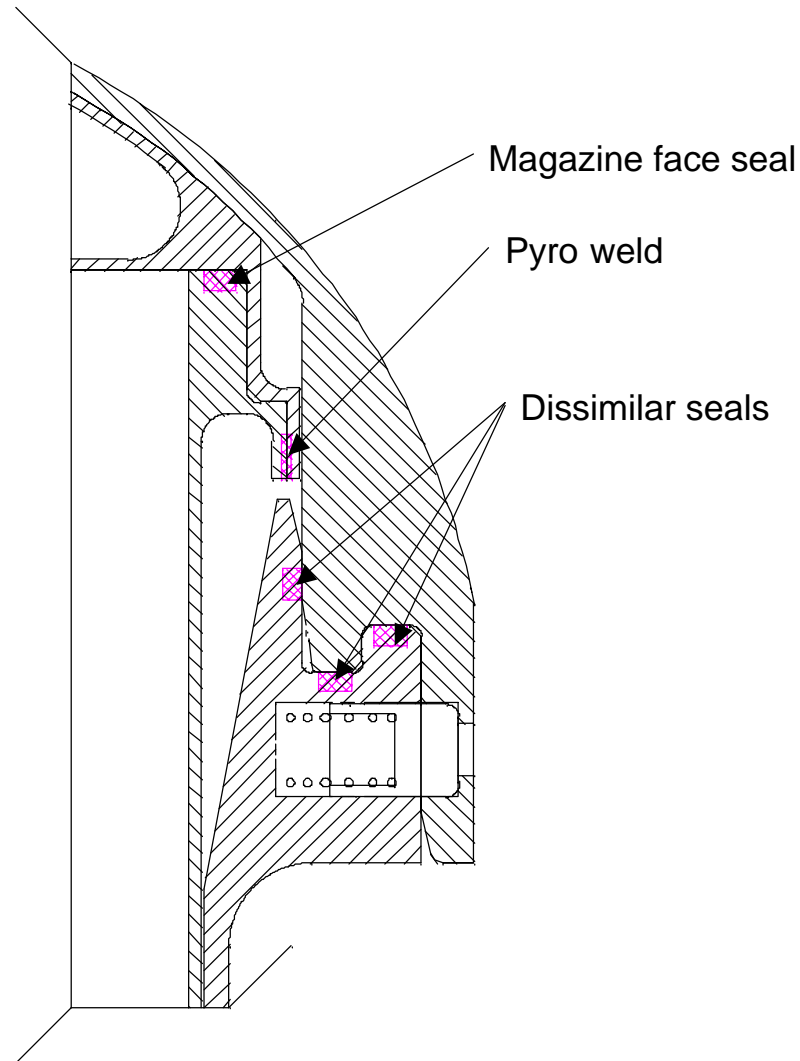
Risk-based Magazine Concept



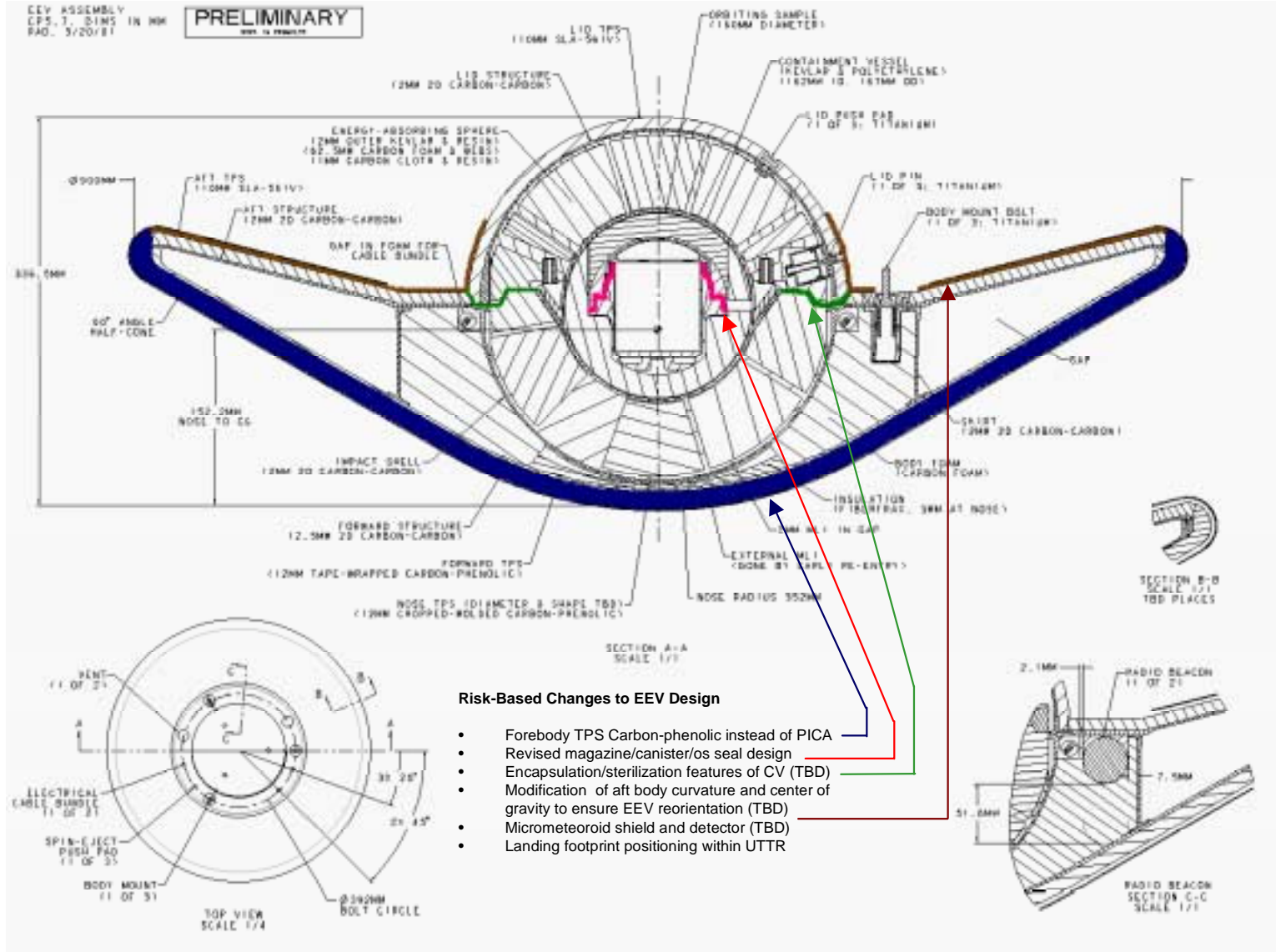
Magazine in Sealed Position

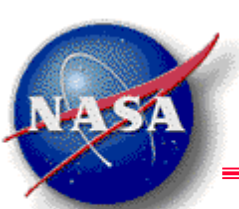


Detail of Risk-Based Sealing



PRA-Based EEV Design Changes.





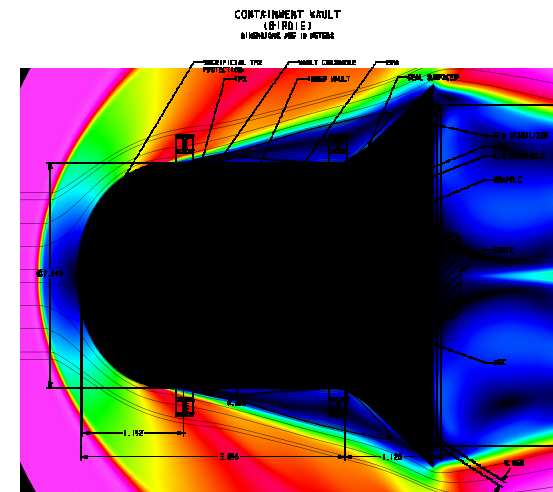
Phase 7: Hypersonic Entry

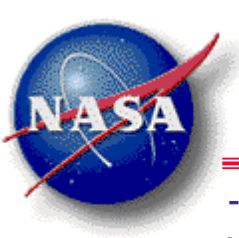
WAS:

- Implemented mitigators
 - ERV spacecraft packaged in a vault in the shuttle payload bay
 - Vault will come free of the shuttle during aerodynamic break-up
 - Vault has sacrificial layer to sustain break-up collisions, and TPS for travel through heat pulse
 - Vault has a multi-shell design with crushable impact absorbing material and a parachute to descend slowly
 - Vault will float if free from the shuttle and in water, but is designed to ~6000 m pressure if undamaged
- Other potential mitigators
 - Flotation Device can be added to further assure flotation
 - “Poison pill” can be added to sterilize samples
 - Better understanding vault response to hypersonic breakup scenarios

IS:

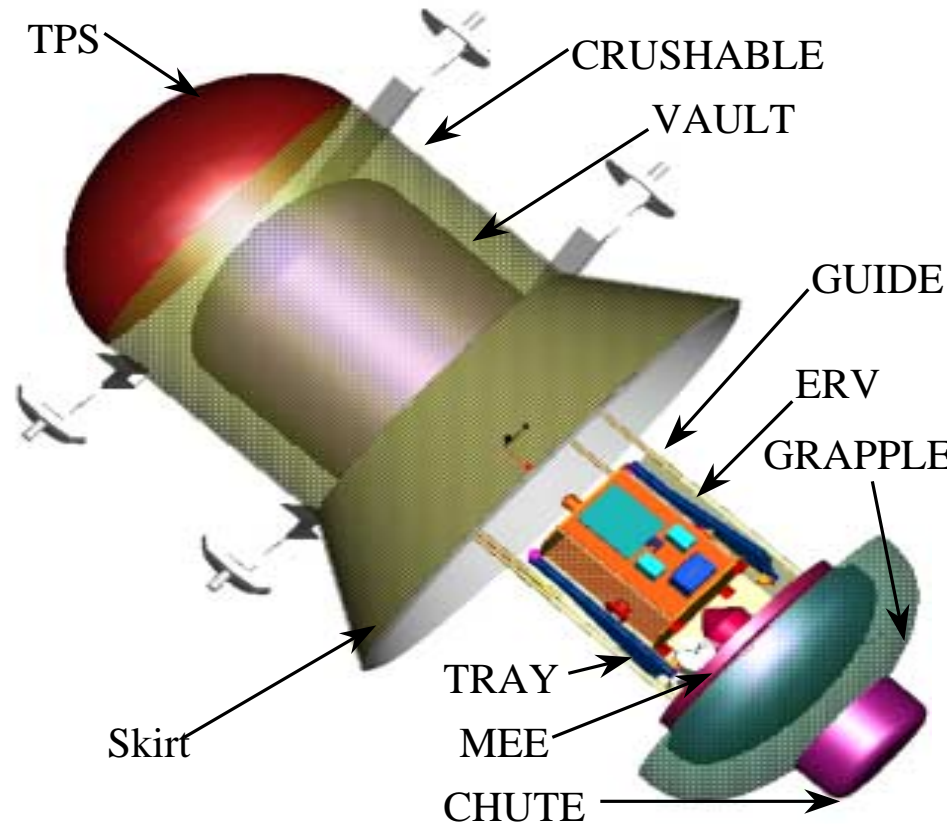
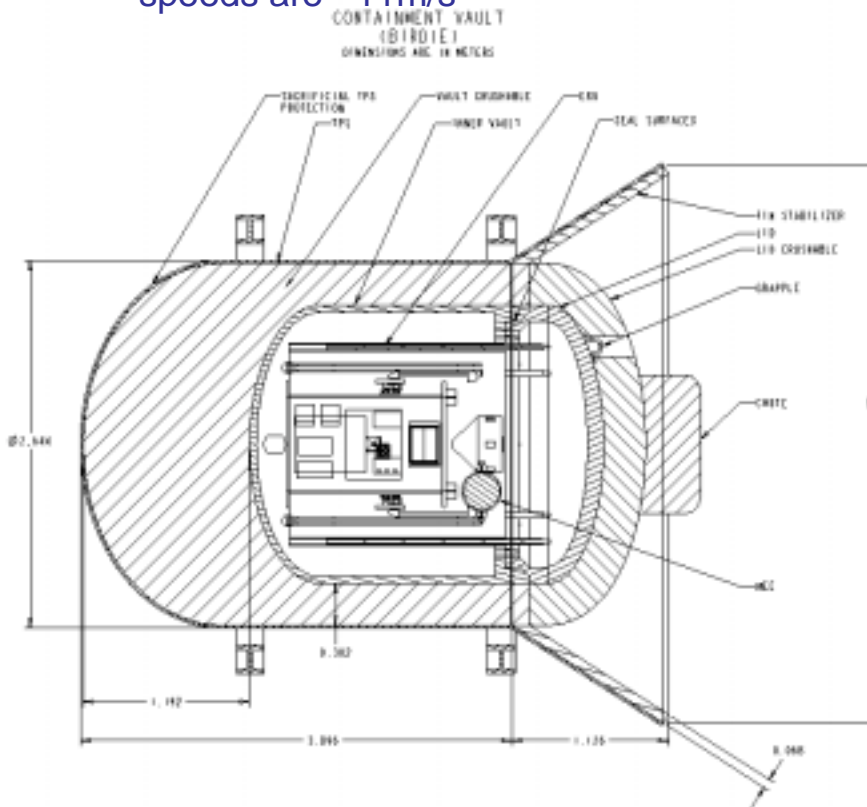
- Potential mitigators
 - Increase shuttle deorbit burn reliability
 - Implement intervention to recover vault from hostile territory





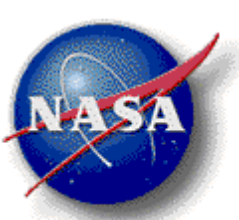
Vault Design

-For cases of Aerodynamic break-up the vault need only slow down aerodynamically to velocities required for the chute to deploy. The current design satisfies this by aerodynamically slowing down to ~Mach 0.5. Parachute landing speeds are ~11m/s



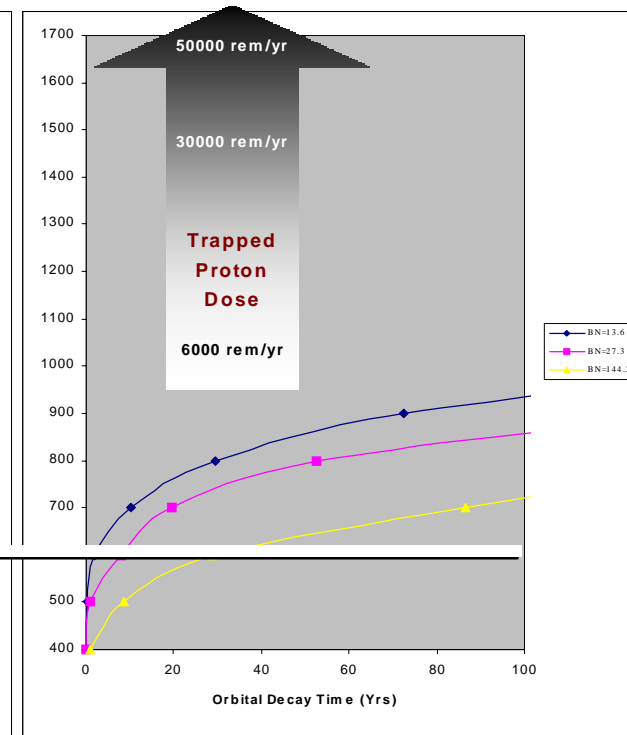
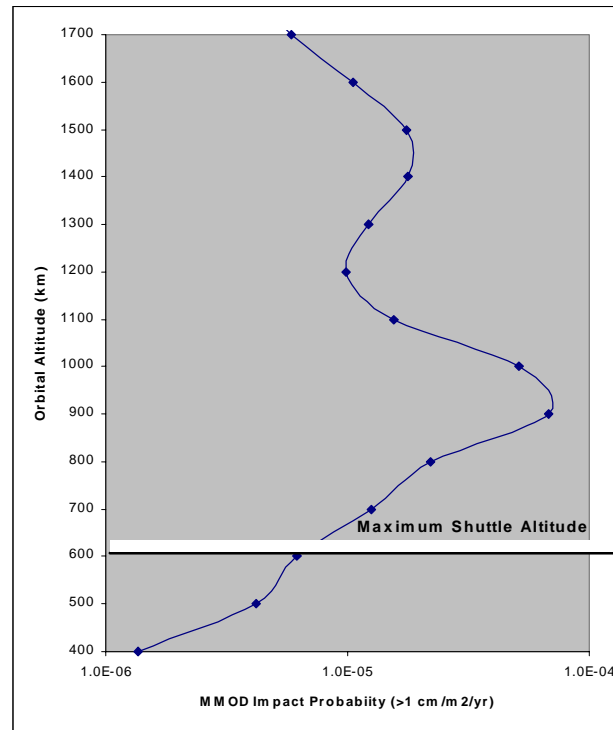
Total Mass: 10400 kg

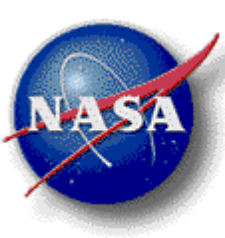
Inner Vault & Mechanisms:
2600 kg



Phase 1: Above Safe Orbit

- No CNA events above “safe” orbit.
 - Above “safe orbit”, metric is mission success
- A safe orbit is a trade among orbital lifetime, orbital debris and radiation flux
 - 500-700 km best for OD avoidance
 - Orbital lifetime in tens of years (e.g. HST orbit)
 - 700-1000 km worst OD zone
 - Most “100-year orbits” fall in this zone
 - 1200 km would be a “desirable” disposal altitude
 - There is a drop-off in OD after this altitude
 - Very long lifetime orbits

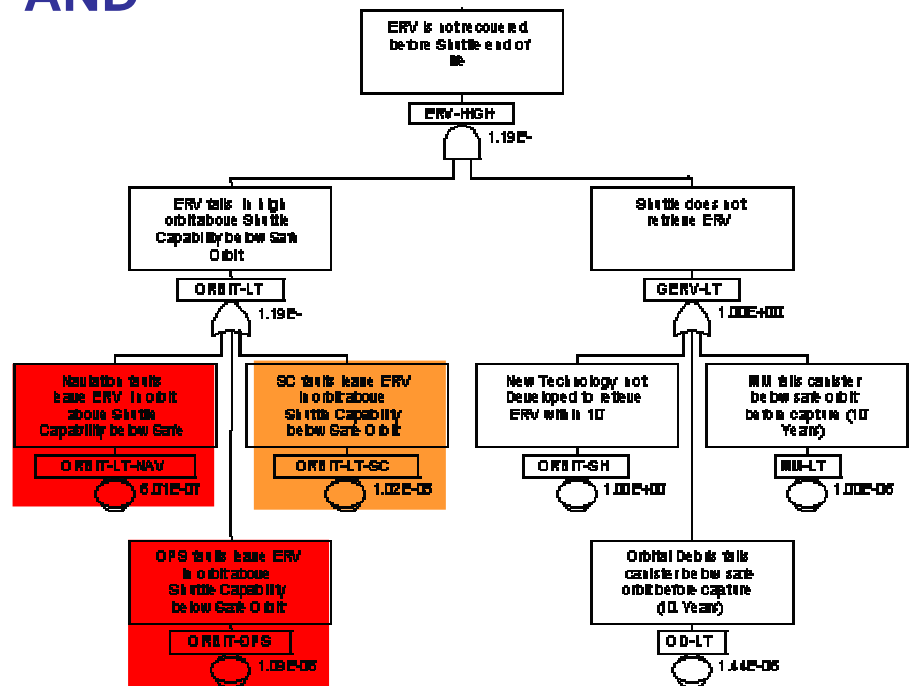




Phase 2: ERV Below Safe Earth Orbit

Risk Drivers:

- ERV fault leaves it below safe orbit, but above shuttle orbit
- AND**
- New technology not developed to retrieve ERV within 10 years
- AND**
- MM or OD fails canister



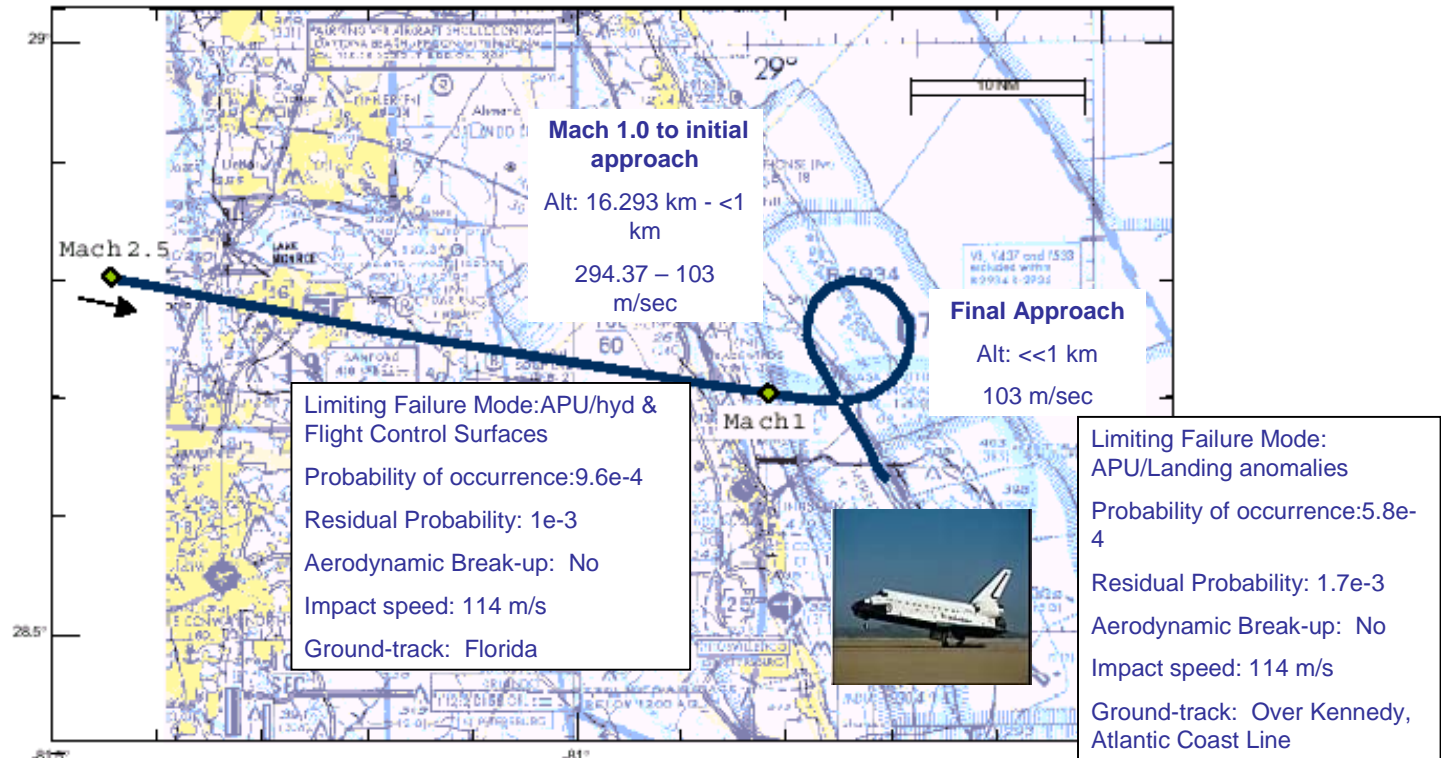


Impact Velocities

The Impact Velocity of an Intact Shuttle was taken from:

Galileo: Uncontrolled STS Orbiter Re-entry- A. McRonald, JPL

- 114 m/s was quantified as the worst case for an out of control orbiter falling at speeds that would allow it to remain intact
- JSC Flight Dynamics Division reviewed the document and concurs with this number.





Phase 9: Landing

Risk driver:

- Orbiter failure during landing

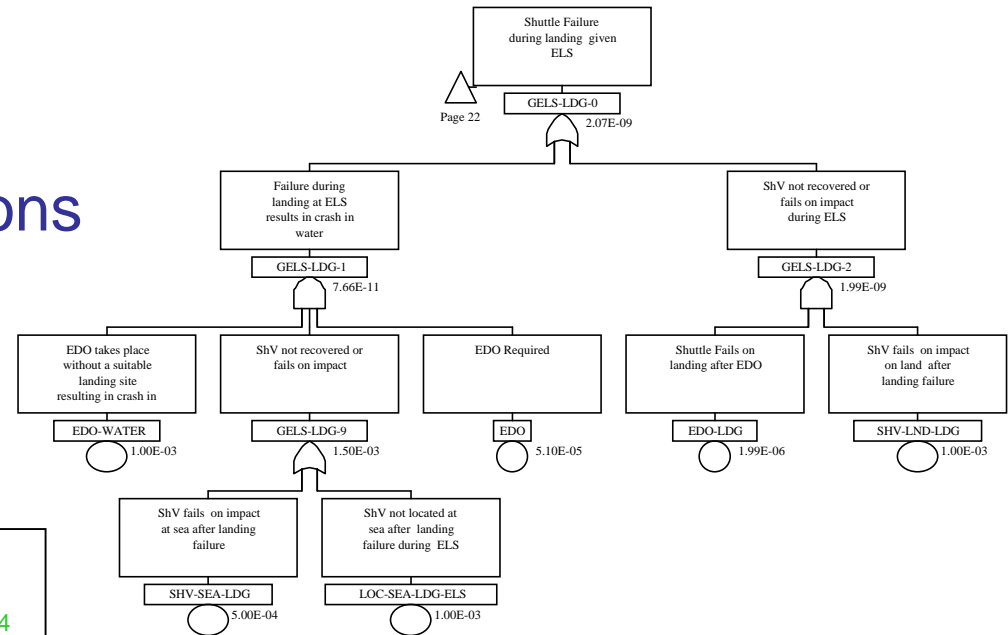
AND

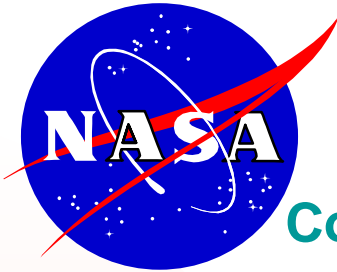
- Vault failure during exposure to Orbiter landing impact conditions



Final Approach
 Alt: <<1 km
 103 m/sec

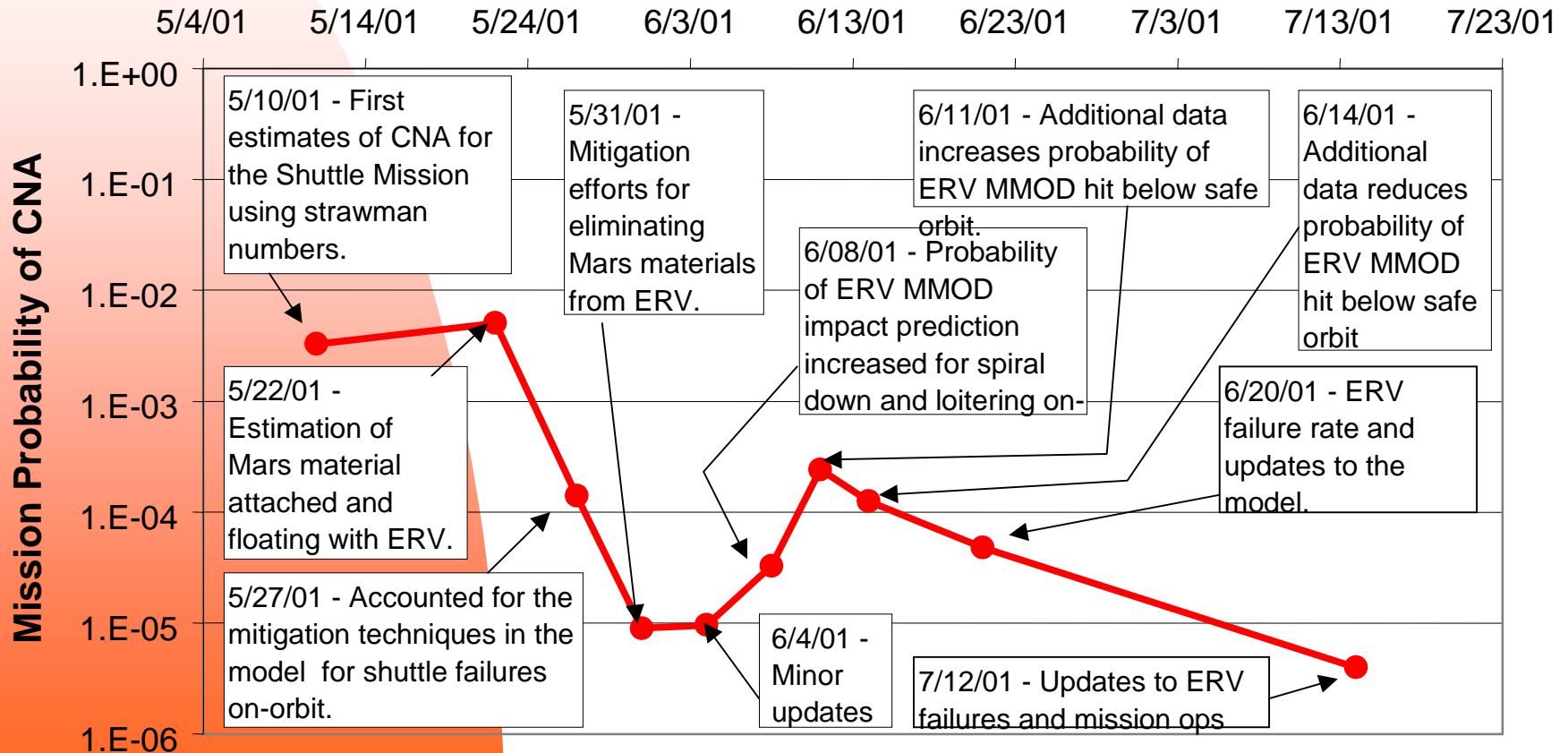
Limiting Failure Mode:
 APU/Landing anomalies
 Probability of occurrence: 5.8e-4
 Residual Probability: 1.7e-3
 Aerodynamic Break-up: No
 Impact speed: 114 m/s
 Ground-track: Over Kennedy,
 Atlantic Coast Line

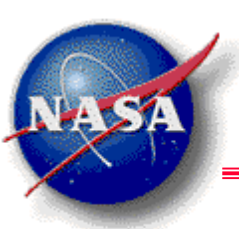




Containment Not Assured (CNA) for Shuttle Mission Running Probability During Conceptual Design

Design Session Dates





Summary

- Risk-based design is appropriate for many segments of the MSR mission
- PRA's make the design team carefully think through the problem
- PRA results focused the design effort
 - Constant iteration among design team and risk analysts
- PRA results constantly shifted with changes in the design. Real time PRA tools required to allow currency with new design environment
- Concurrent design and PRA allowed expected design risk to be tracked as a design resource
- Overall Risk Based design approach implementation considered a success

