Assessing the Risks of Space Exploration

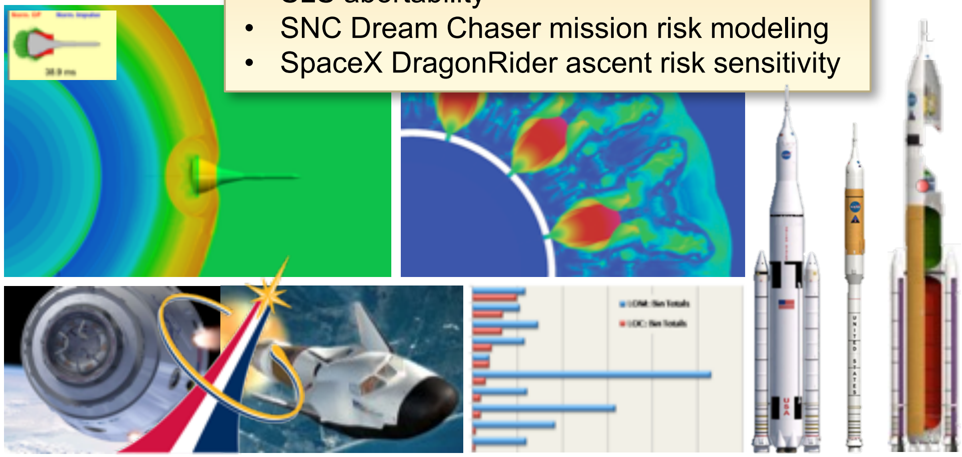
Donovan Mathias
Engineering Risk Assessment (ERA) Team
NASA Advanced Supercomputing Division
NASA Ames Research Center

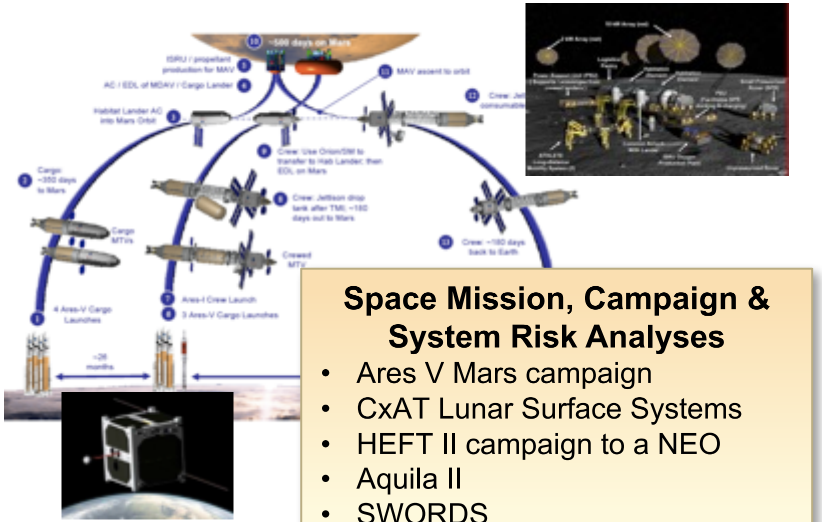
Surviving Space
Stanford University
March 1, 2018

Engineering Risk Assessment

Crew Launch Vehicle Risk Assessment & Risk-Informed Design

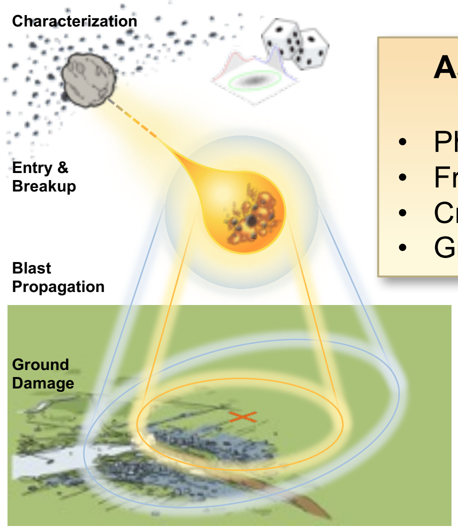
- Ares I/V integrated LOM/LOC
- SLS abortability
- SNC Dream Chaser mission risk modeling
- SpaceX DragonRider ascent risk sensitivity





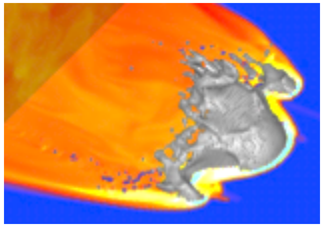
Space Mission, Campaign & System Risk Analyses

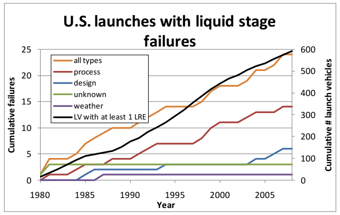
- Ares V Mars campaign
- CxAT Lunar Surface Systems
- HEFT II campaign to a NEO
- Aquila II
- SWORDS

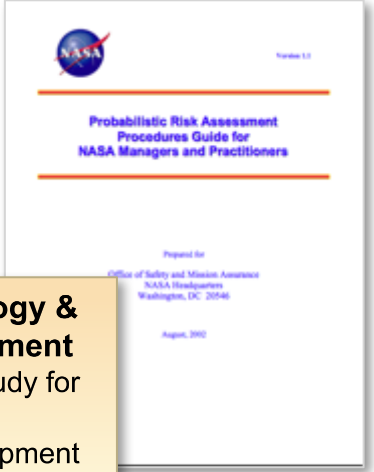


Asteroid Threat Assessment Project (ATAP)

- Physics-based impact risk model
- Fragmentation/breakup
- Crater-forming impact
- Ground damage assessment







Version 1.1

Probabilistic Risk Assessment Procedures Guide for NASA Managers and Practitioners

Prepared for

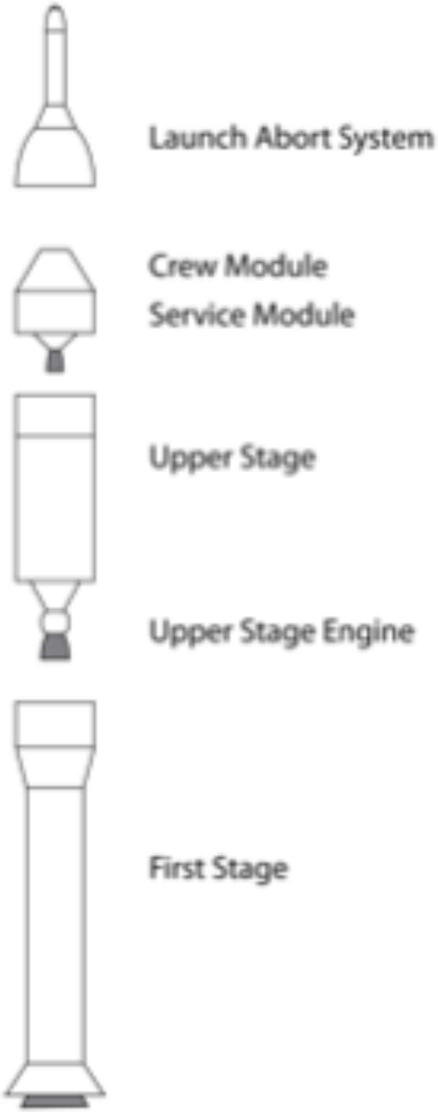
Office of Safety and Mission Assurance
NASA Headquarters
Washington, DC 20546

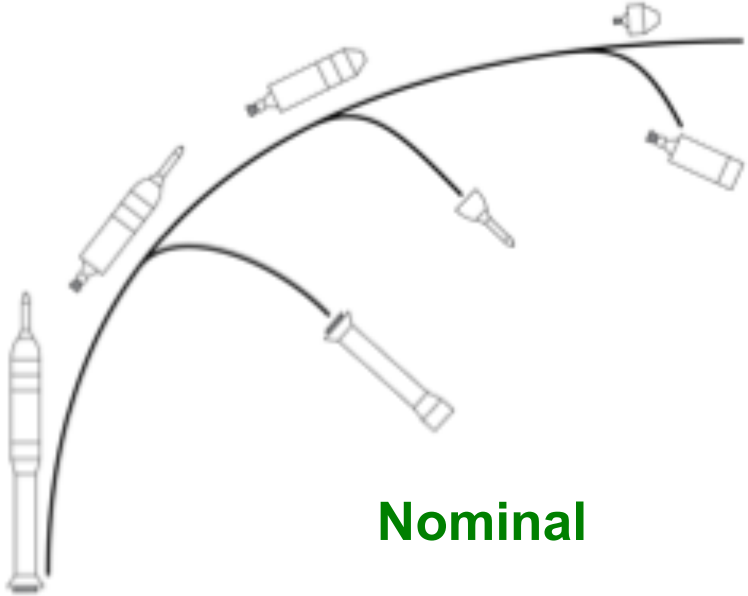
August, 2002

Agency Risk Methodology & Requirements Development

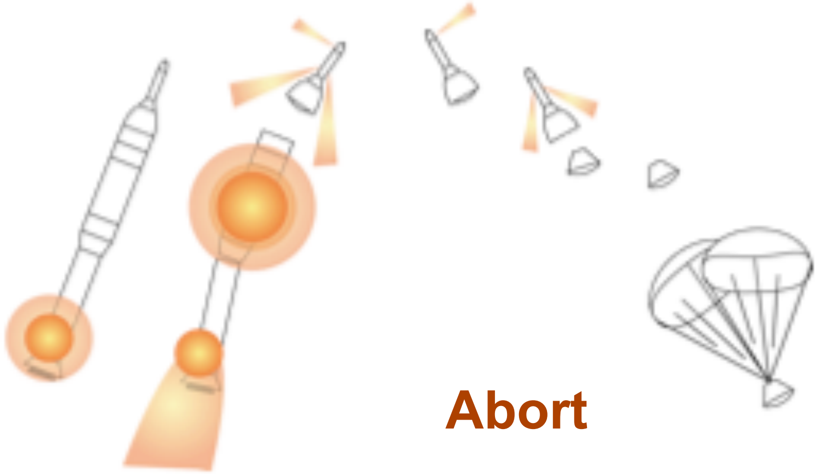
- Liquid/Solid Propellant Study for NASA's Study of Rockets
- CCP requirements development
- OSMA PRA guide chapters and training modules.

Example Architecture



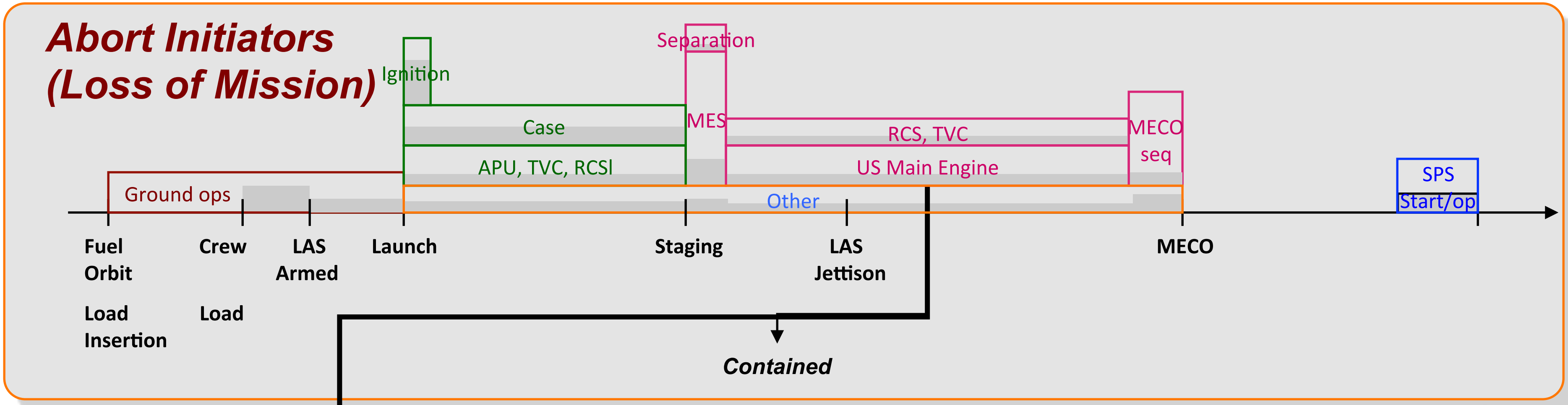


Nominal

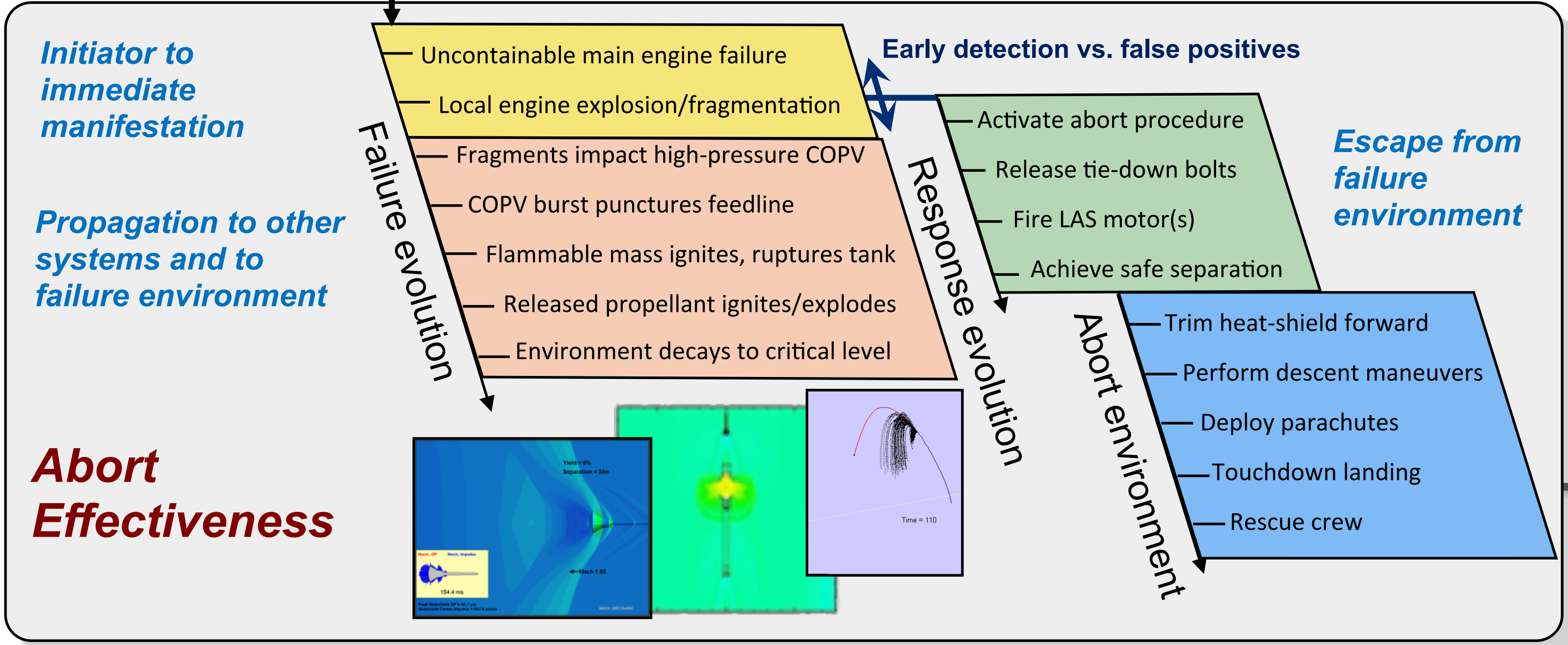


Abort

Integrated Ascent Risk Modeling



Abort Initiators (Loss of Mission)



Initiator to immediate manifestation

- Uncontainable main engine failure
- Local engine explosion/fragmentation

Early detection vs. false positives

Propagation to other systems and to failure environment

- Fragments impact high-pressure COPV
- COPV burst punctures feedline
- Flammable mass ignites, ruptures tank
- Released propellant ignites/explodes
- Environment decays to critical level

- Activate abort procedure
- Release tie-down bolts
- Fire LAS motor(s)
- Achieve safe separation

Escape from failure environment

- Trim heat-shield forward
- Perform descent maneuvers
- Deploy parachutes
- Touchdown landing
- Rescue crew

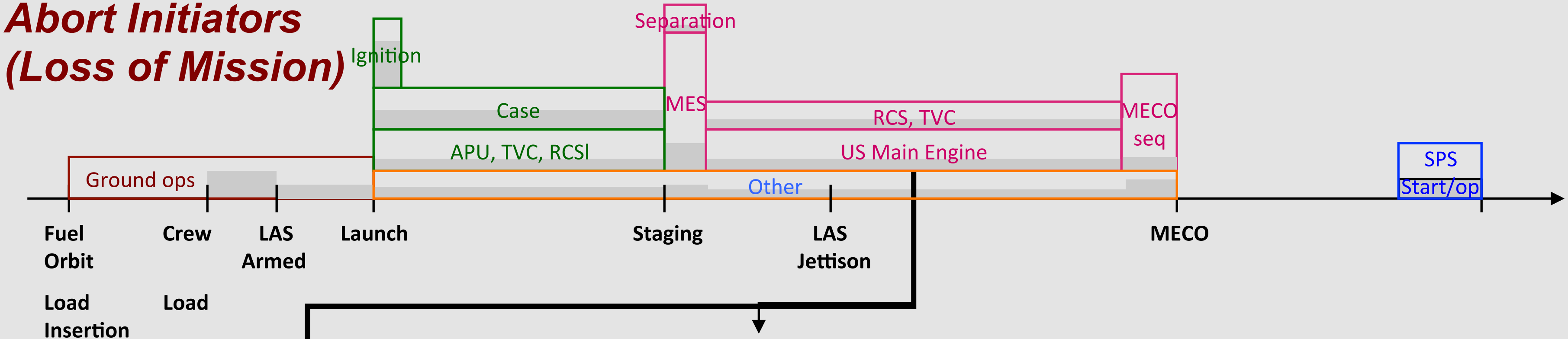
Abort Effectiveness

LOM

LOC

Integrated Ascent Risk Modeling

Abort Initiators (Loss of Mission)



Ignition

Case

APU, TVC, RCSl

Separation

MES

RCS, TVC

US Main Engine

MECO seq

Ground ops

Other

SPS Start/op

Fuel Orbit

Crew

LAS Armed

Launch

Staging

LAS Jettison

MECO

Load Insertion

Load

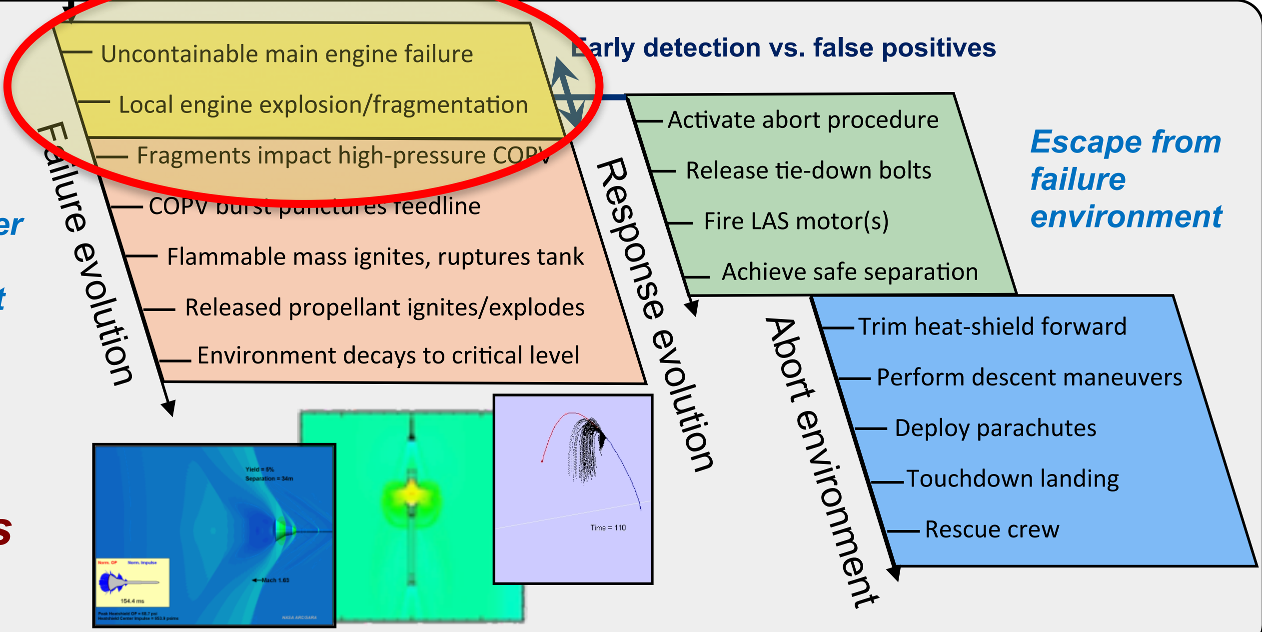
Contained

LOM

Initiator to immediate manifestation

Propagation to other systems and to failure environment

Abort Effectiveness



Failure evolution

- Uncontainable main engine failure
- Local engine explosion/fragmentation
- Fragments impact high-pressure COPV
- COPV burst punctures feedline
- Flammable mass ignites, ruptures tank
- Released propellant ignites/explodes
- Environment decays to critical level

Early detection vs. false positives

Response evolution

- Activate abort procedure
- Release tie-down bolts
- Fire LAS motor(s)
- Achieve safe separation

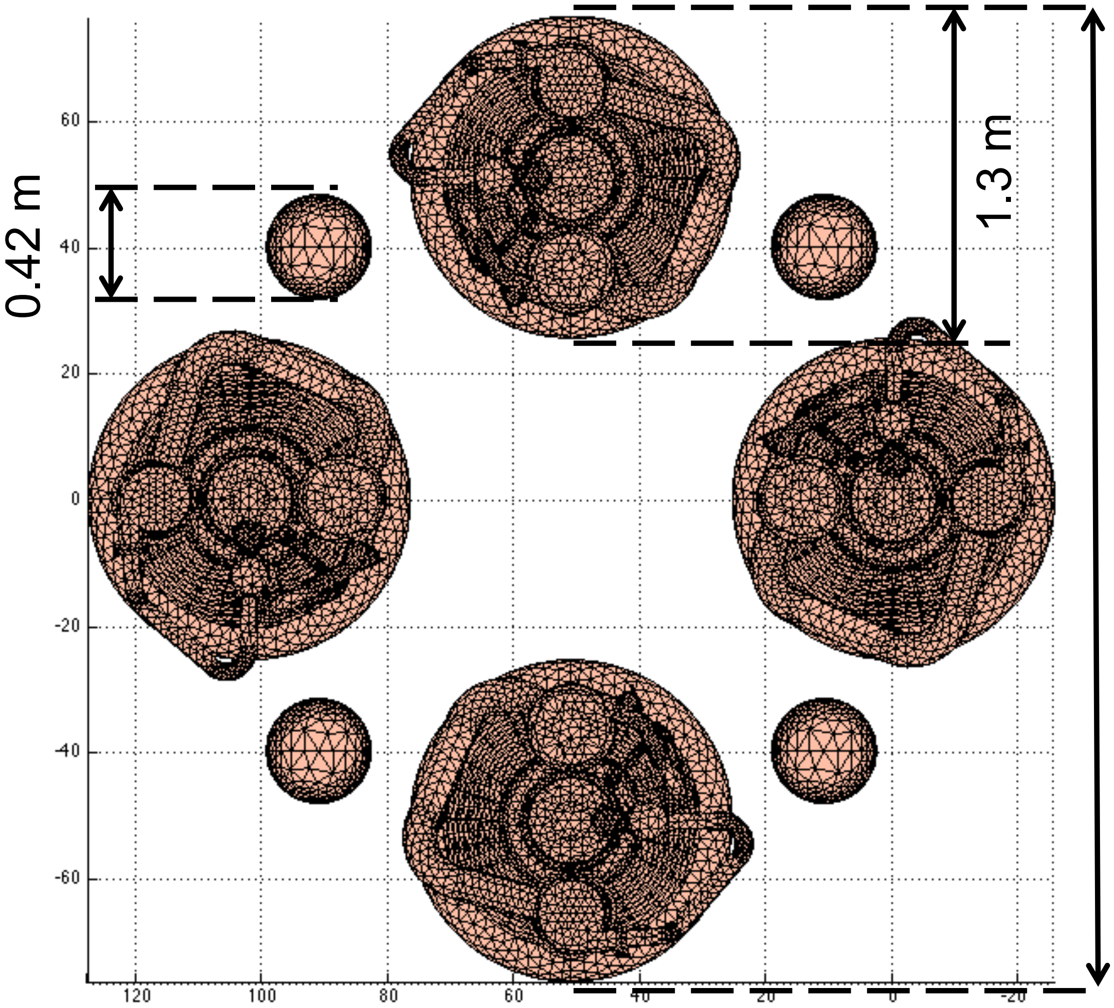
Abort environment

- Trim heat-shield forward
- Perform descent maneuvers
- Deploy parachutes
- Touchdown landing
- Rescue crew

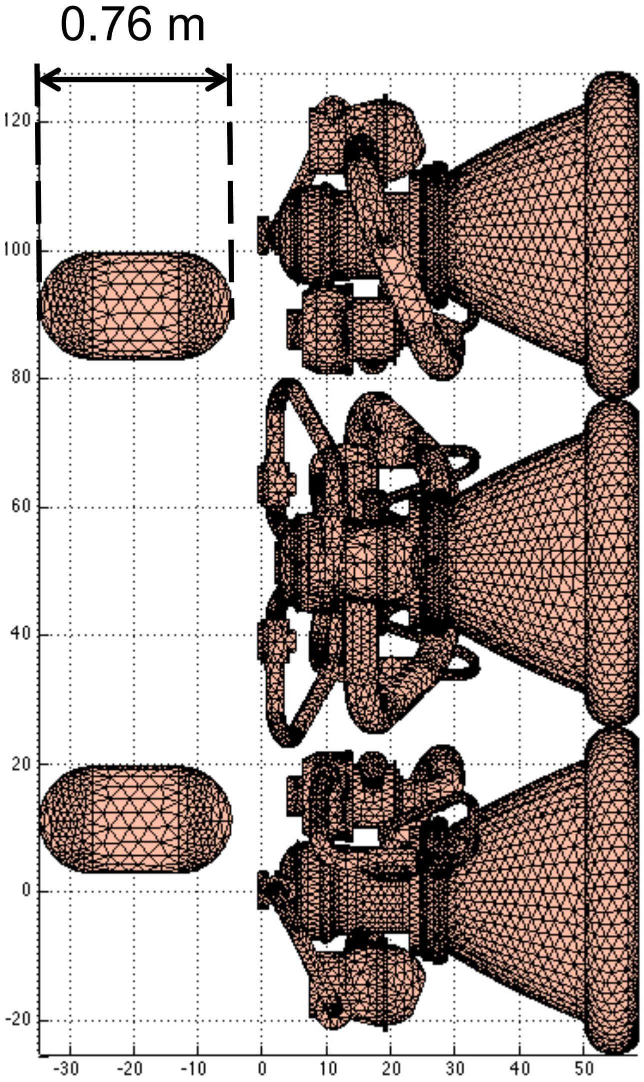
Escape from failure environment

LOC

Test Case Setup



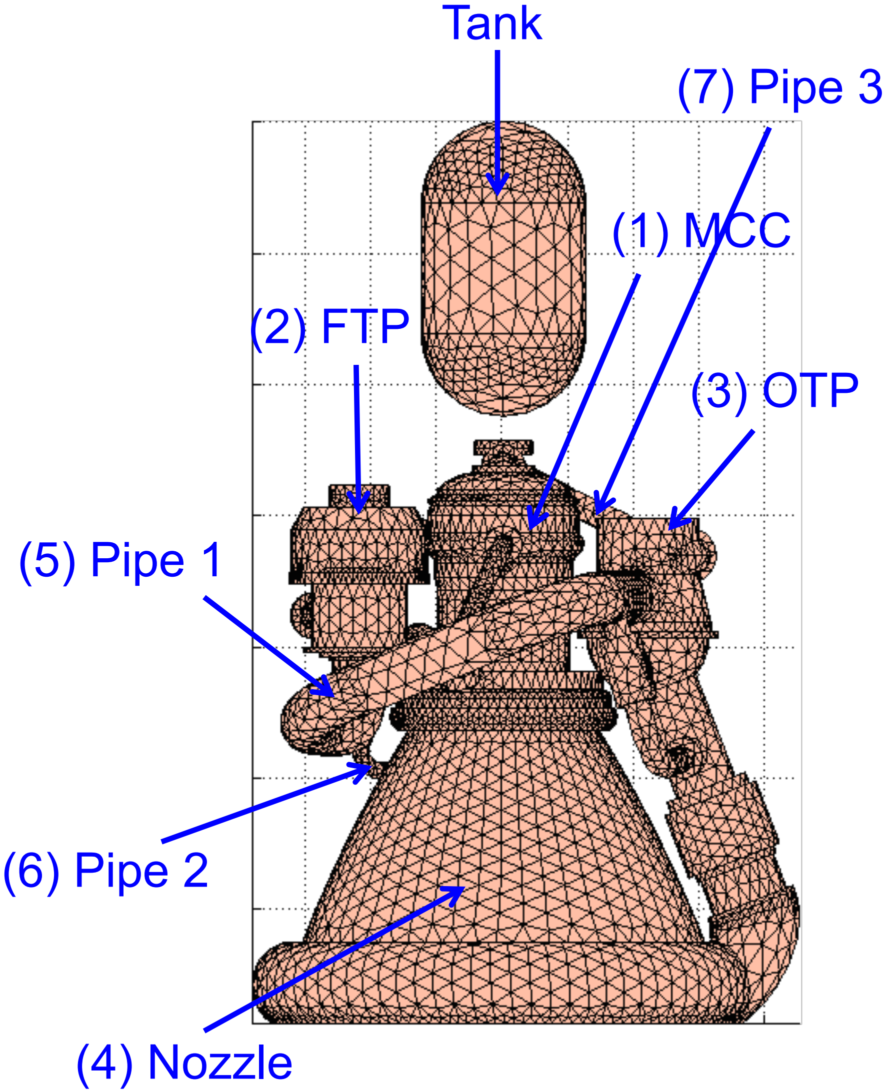
Top Down



Side

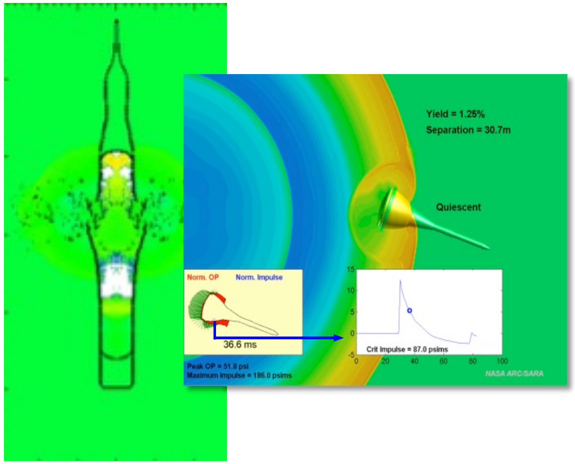
Test Case: 4 Engines + Tanks

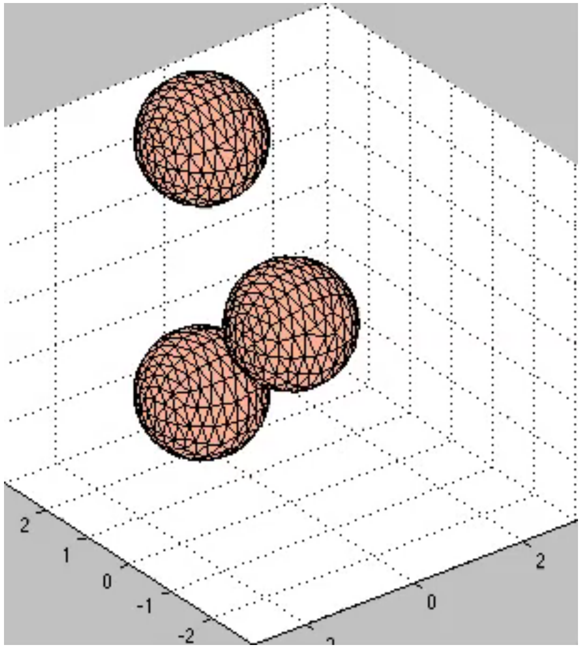
- Simple engine model for generic launch vehicle platform (derived from J2X)
- 32 components: 7 per engine and 4 tanks
  - Main combustion chamber (MCC)
  - 2 turbopumps: fuel (FTP) and oxidizer (OTP)
  - 3 pipes (fuel, oxidizer, hot gas)
  - Nozzle
- Between ~1k–6k triangles per component
- 3 different initiators: MCC, FTP, and OTP



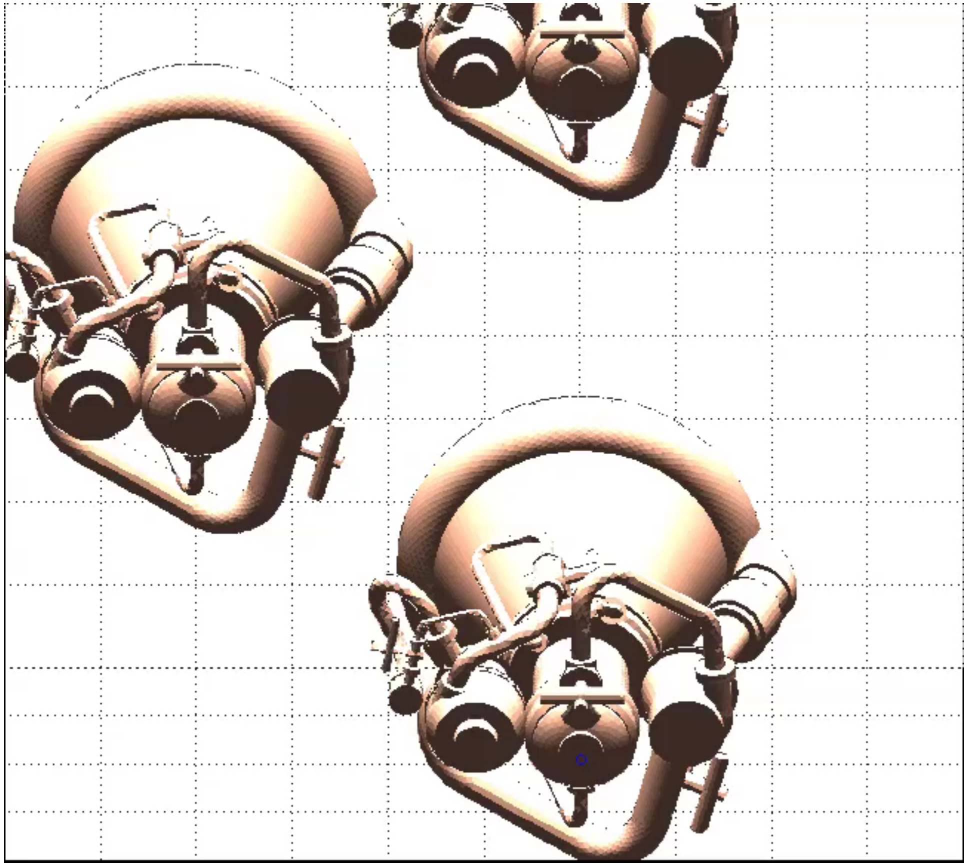
Failure Propagation Model

- Models failure propagation of debris field and blast wave environments
- Consists of component-to-component interactions and behaviors given initial conditions
- Uses Monte Carlo framework developed in C++:
  - Execution begins by seeding a failure and letting it cascade until propagation ends
  - Results include probabilities of component vulnerabilities and scenario tracking
- 100,000 realizations run in ~2 minutes on laptop for current test case

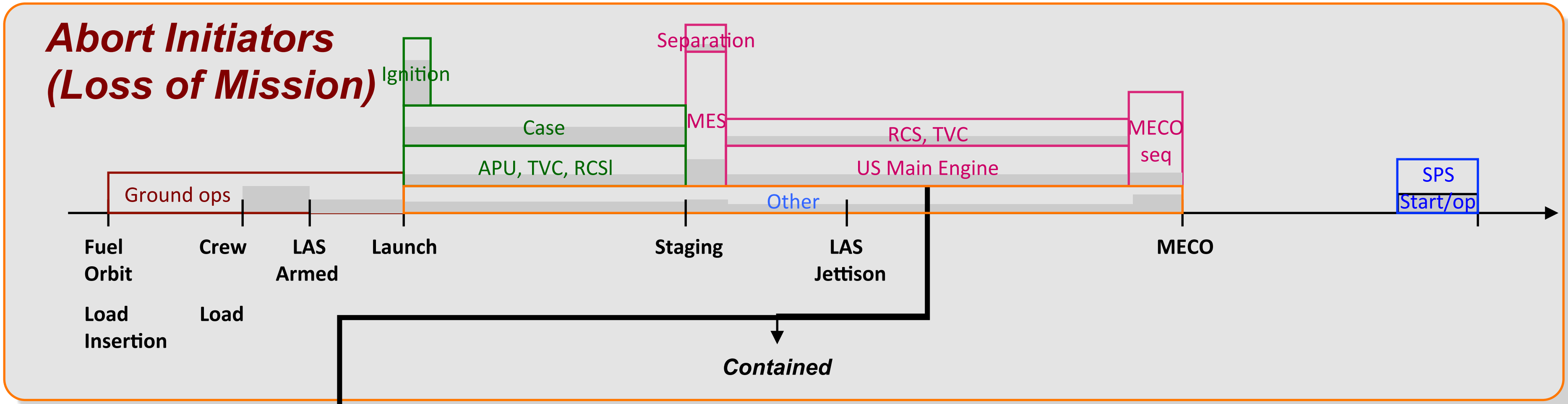




Propagation Example



Integrated Ascent Risk Modeling



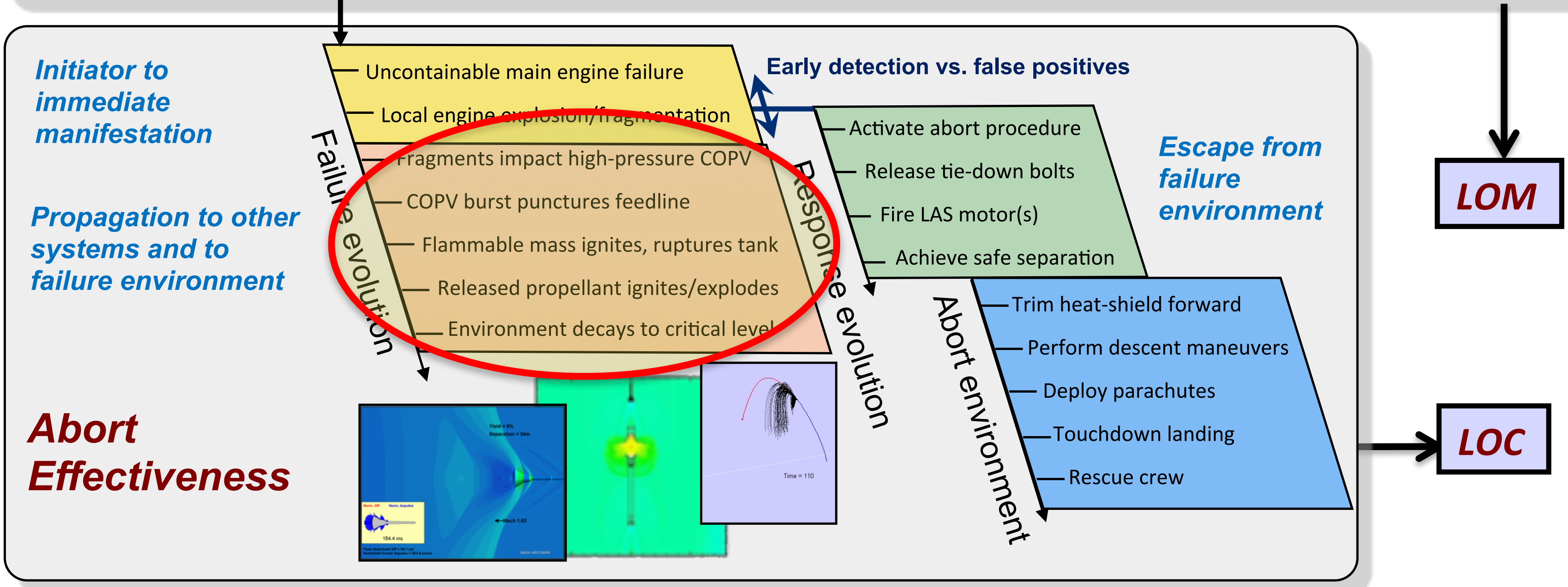
Abort Initiators (Loss of Mission)

Ground ops
Ignition
Case
APU, TVC, RCSl
Separation
MES
RCS, TVC
US Main Engine
MECO seq
Other
SPS Start/op

Fuel Orbit
Crew
LAS Armed
Launch
Staging
LAS Jettison
MECO

Load Insertion
Load

Contained



Initiator to immediate manifestation

Propagation to other systems and to failure environment

Abort Effectiveness

Failure evolution

- Uncontainable main engine failure
- Local engine explosion/fragmentation
- Fragments impact high-pressure COPV
- COPV burst punctures feedline
- Flammable mass ignites, ruptures tank
- Released propellant ignites/explodes
- Environment decays to critical level

Early detection vs. false positives

Response evolution

- Activate abort procedure
- Release tie-down bolts
- Fire LAS motor(s)
- Achieve safe separation

Escape from failure environment

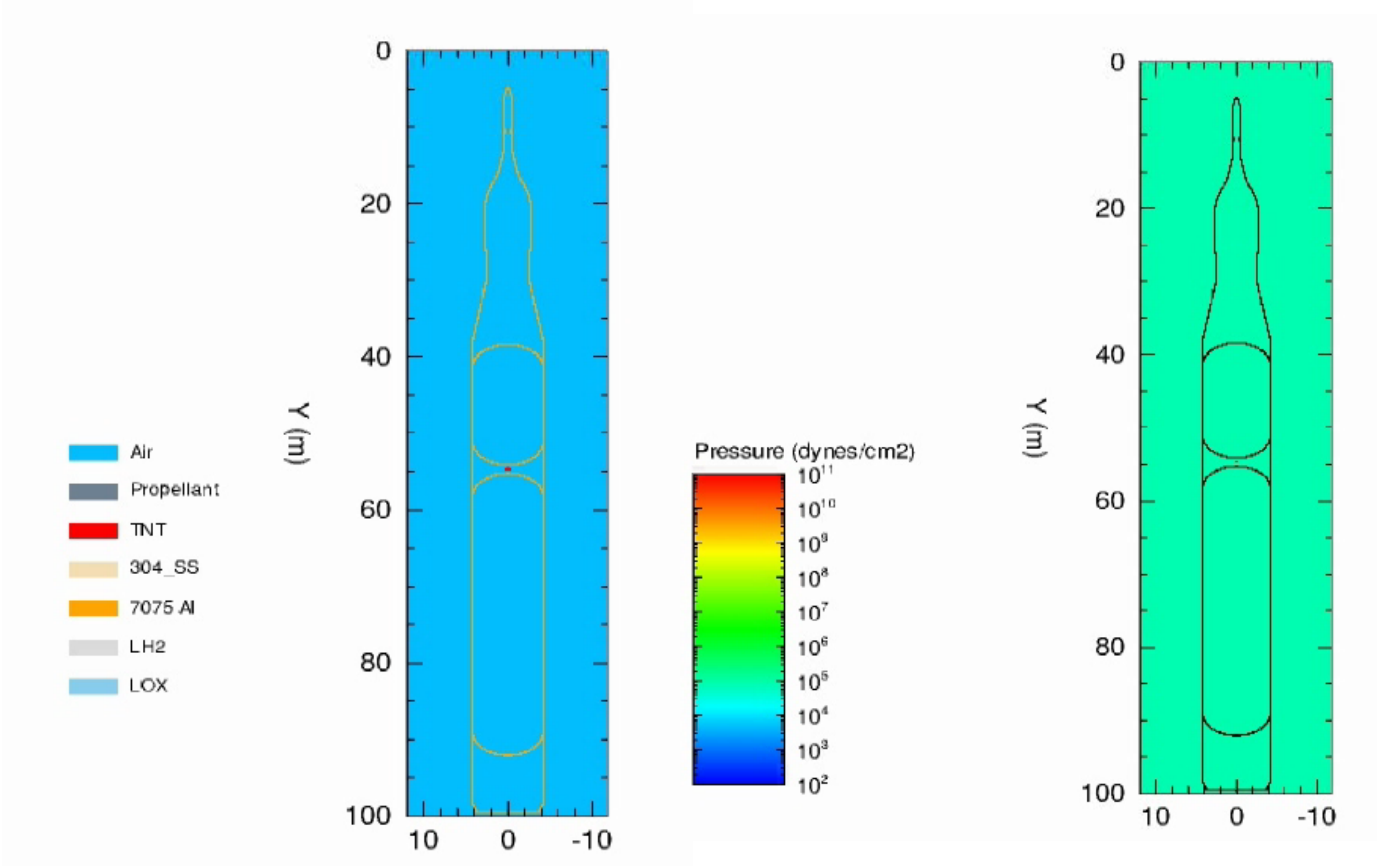
Abort environment

- Trim heat-shield forward
- Perform descent maneuvers
- Deploy parachutes
- Touchdown landing
- Rescue crew

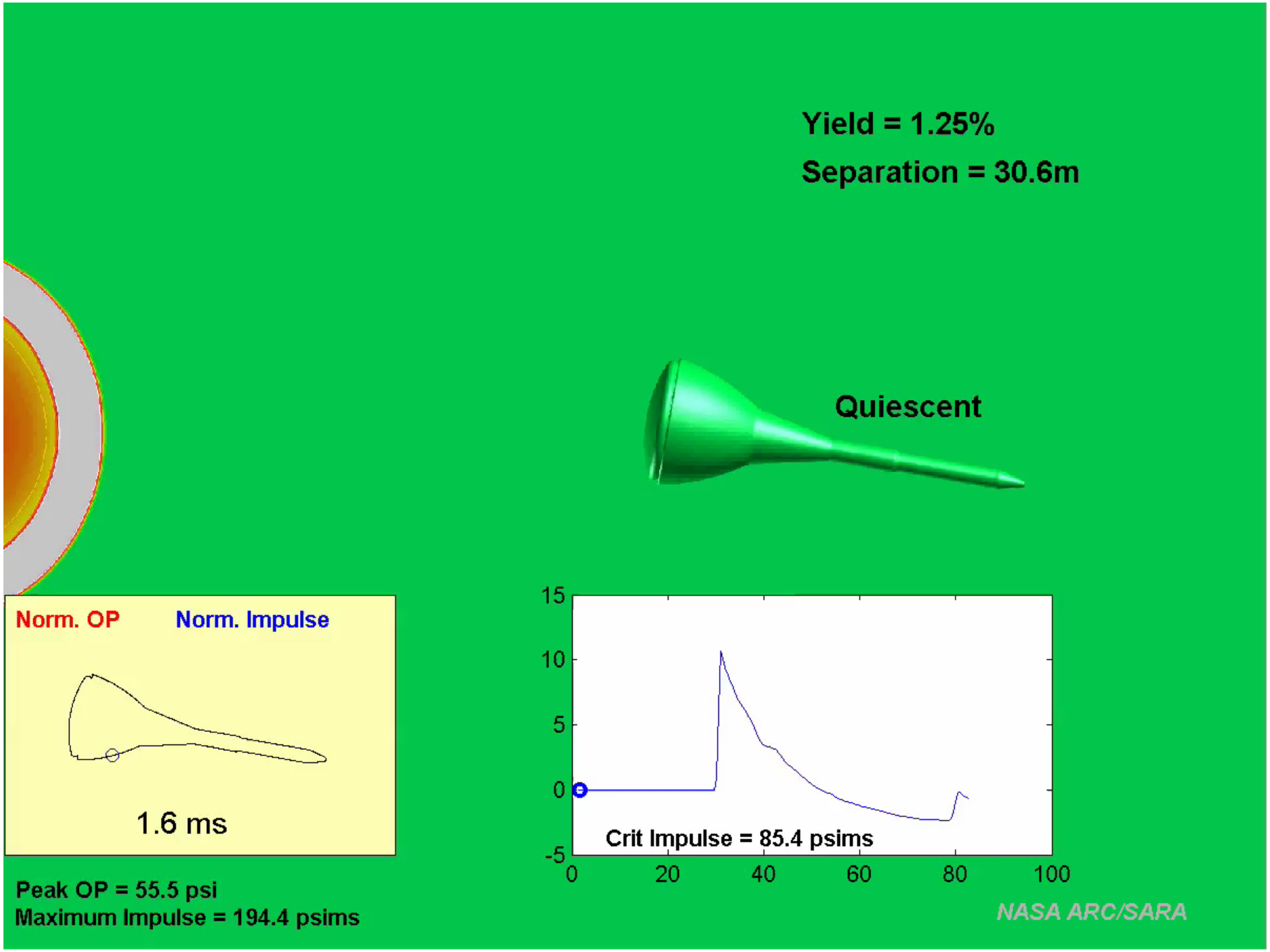
LOM

LOC

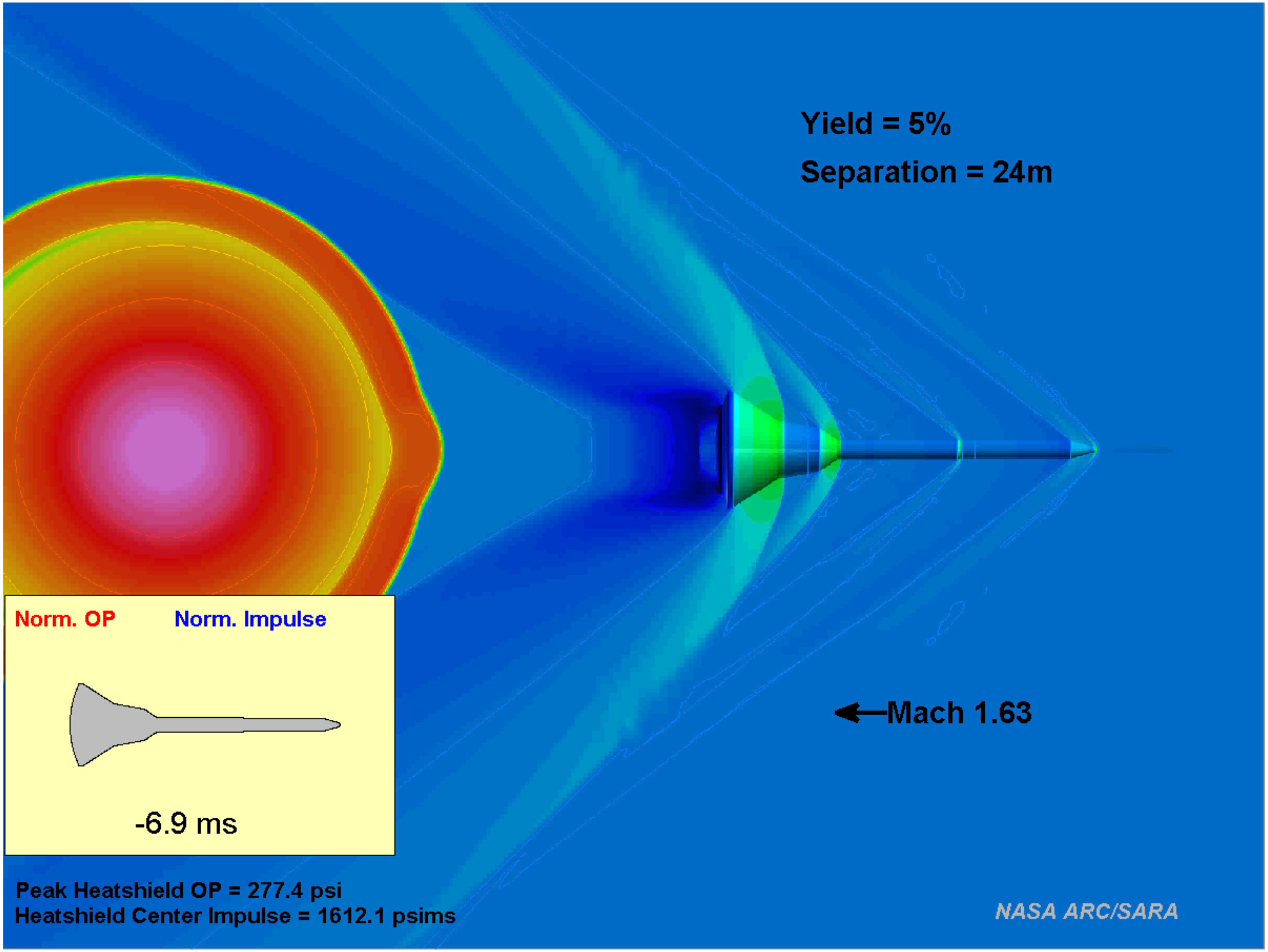
Vehicle-level Explosion Model II



Blast Propagation Model



Blast Propagation Model

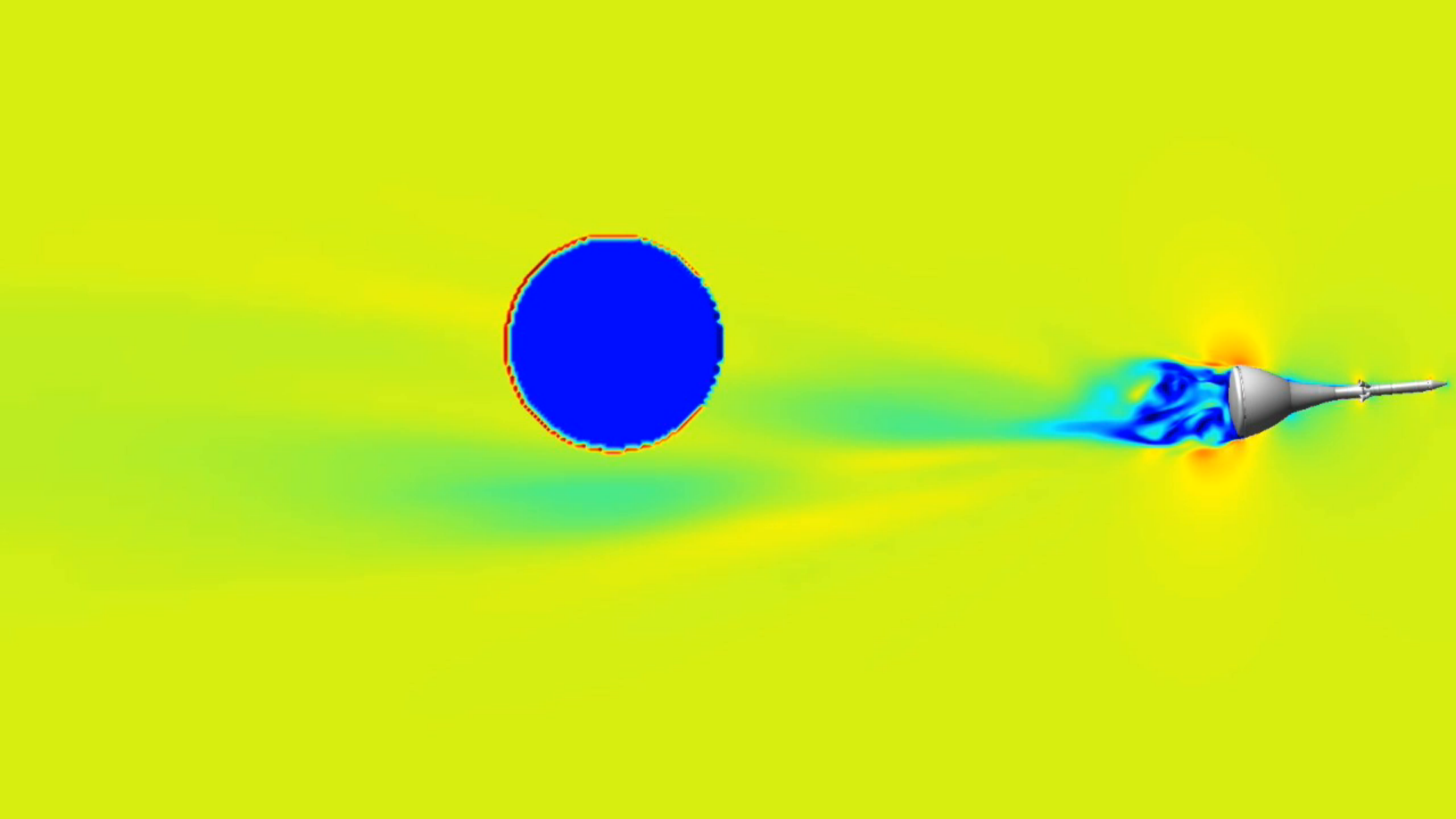


Yield = 5%

Separation = 24m

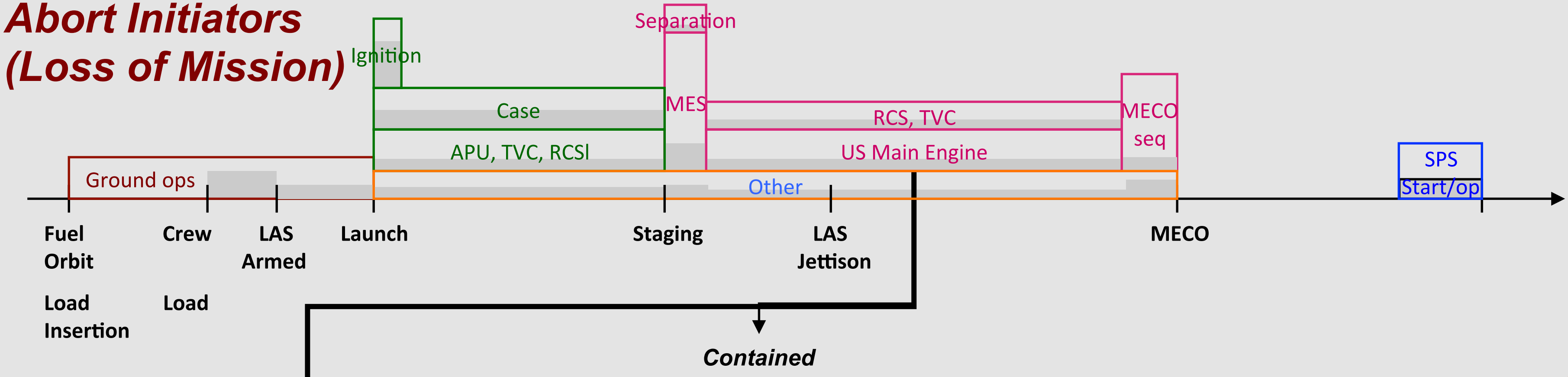
Peak Heatshield OP = 277.4 psi
Heatshield Center Impulse = 1612.1 psims

Blast Propagation Model



Integrated Ascent Risk Modeling

Abort Initiators (Loss of Mission)

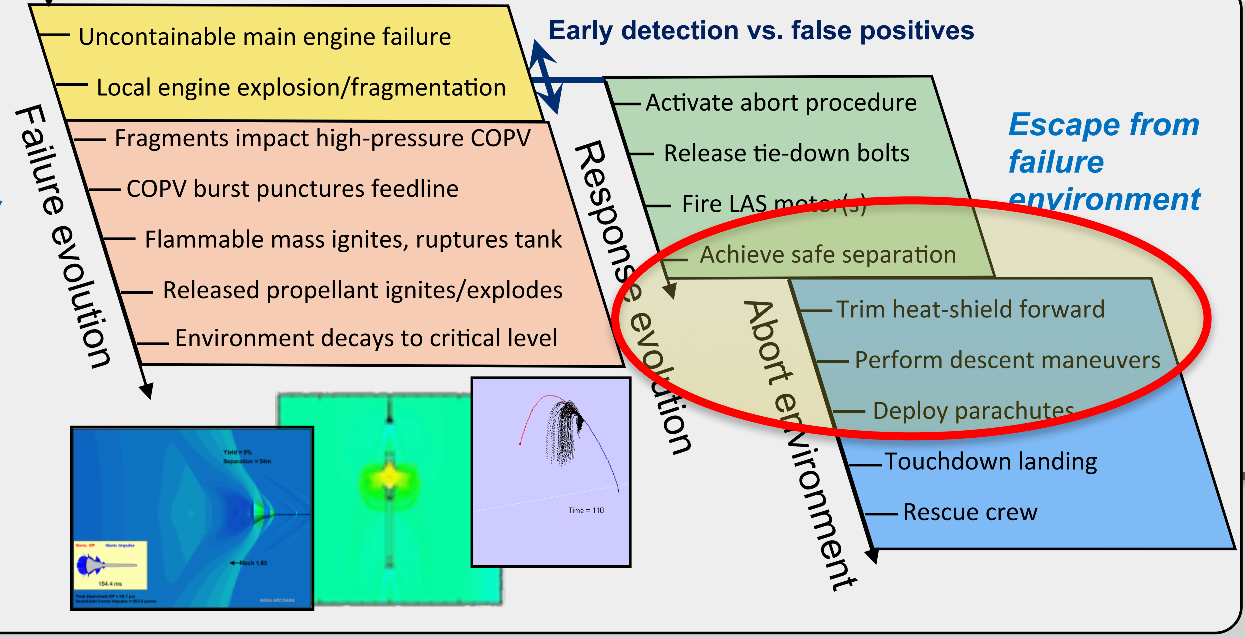


Initiator to immediate manifestation

Propagation to other systems and to failure environment

Escape from failure environment

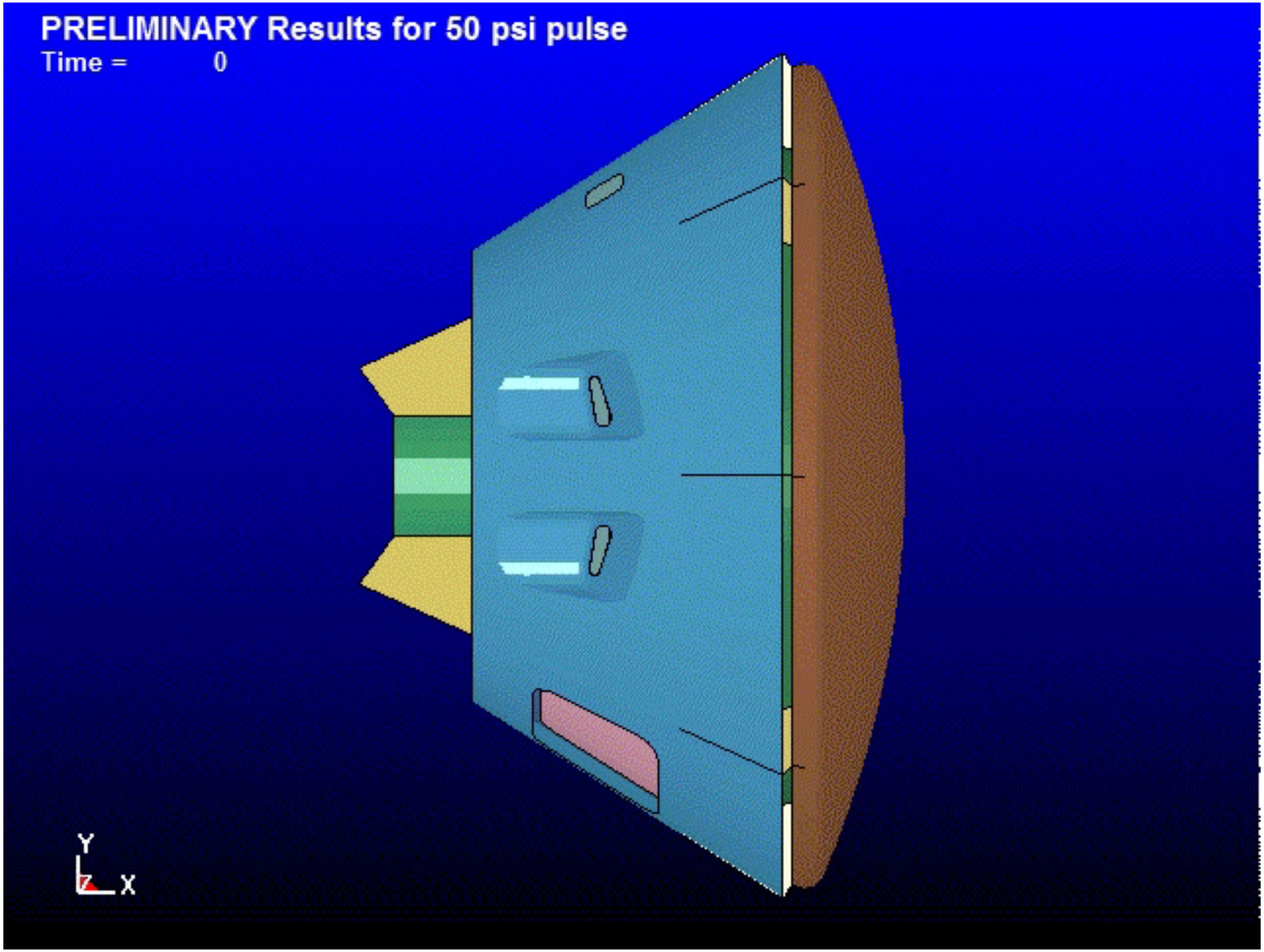
Abort Effectiveness



LOM

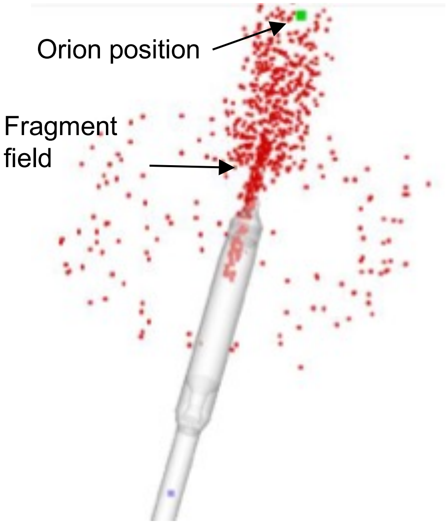
LOC

Structural Response Model

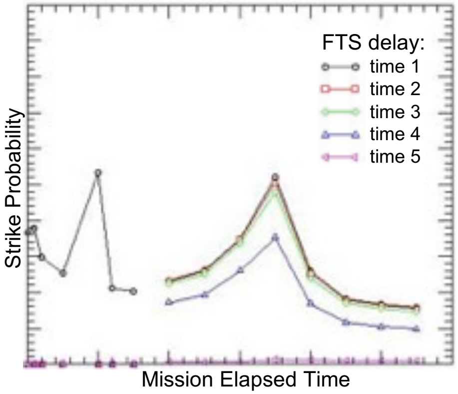


Debris Model

- Debris propagation
  - Three degrees-of-freedom (3DOF) trajectory integration using MISSION code
  - Trajectories calculated for:
    - Launch vehicle
    - Crew module
    - Each fragment of potentially dangerous size
- Initial debris conditions
  - Mass distribution based on experimental data
  - Velocity distribution
    - Experimental and historical data
    - Computed results
- Debris Impact risk determined from intersection of CM and debris trajectories

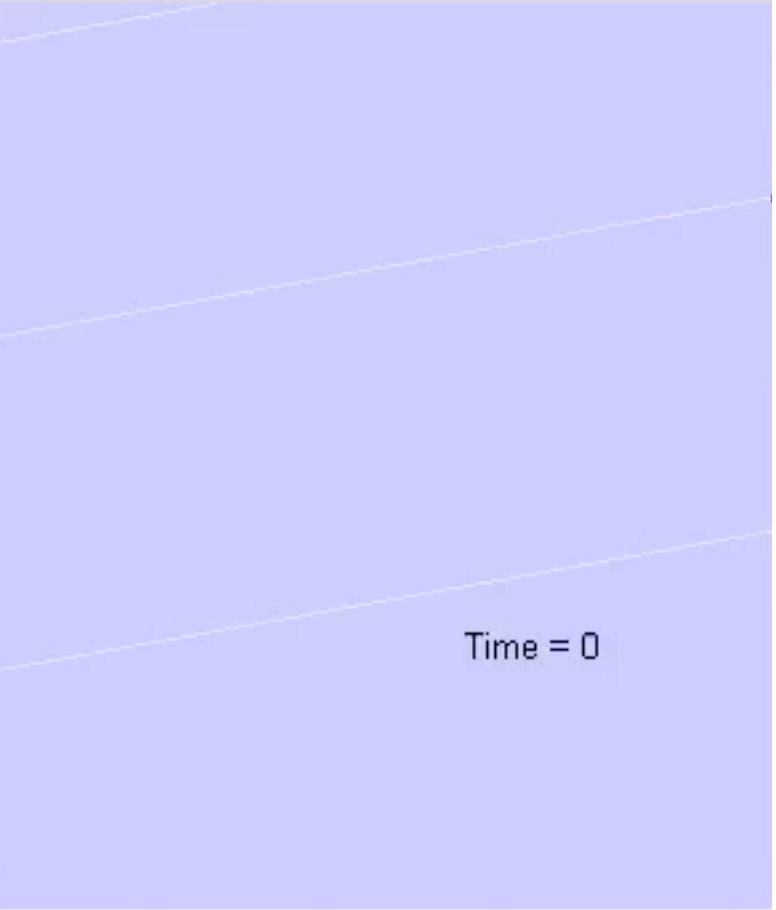


Debris field caused by fragmentation of the Ares I CLV during ascent



Strike probability as a function of MET with penetration criterion

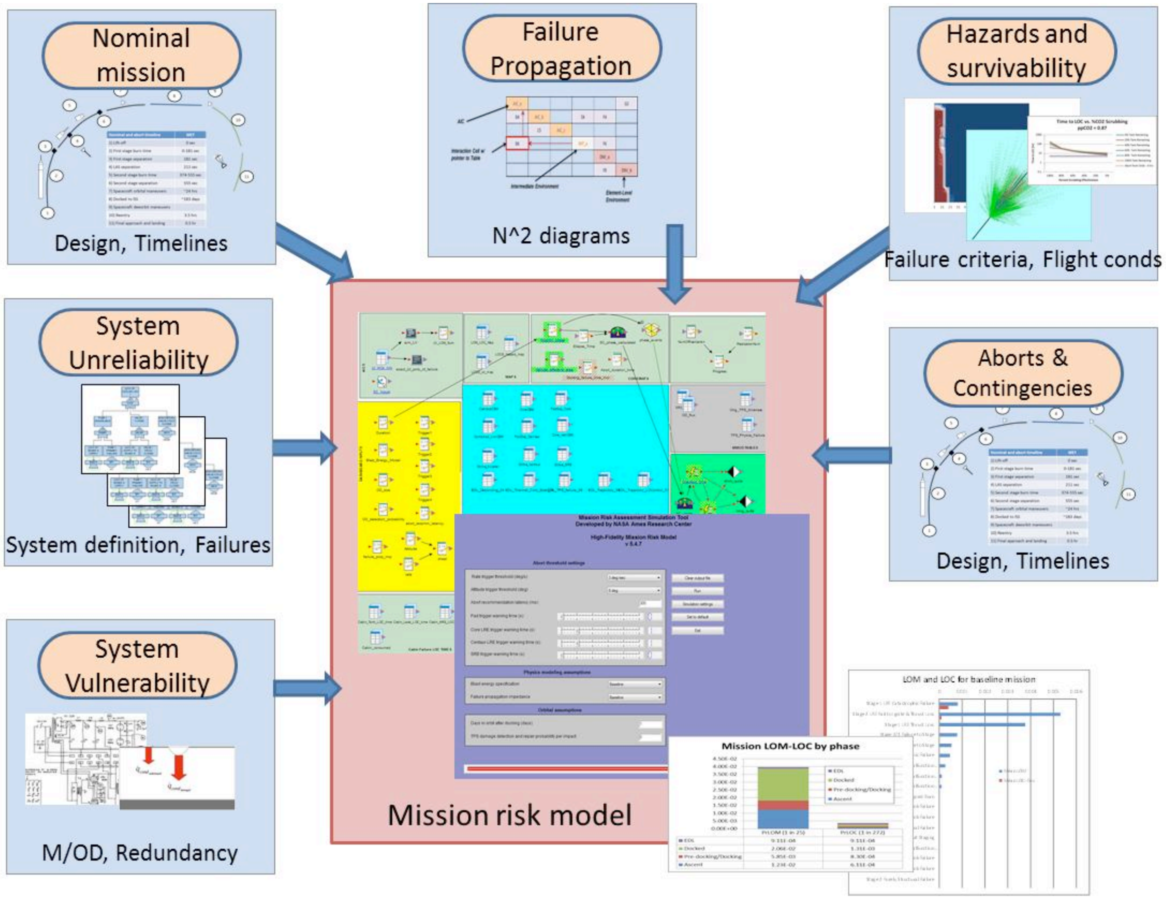
Debris Propagation Model



Risk Contributors

Many contributors to risk as shown below—too many to exhaustively analyze.

- **Physics-based analysis of key risk factors**
  - External hazards
  - Failure environments
- **Dynamic nature of failures**
  - Time dependence
  - State dependence
  - Interactive effects



Nominal mission

Design, Timelines

Failure Propagation

N^2 diagrams

Hazards and survivability

Failure criteria, Flight conds

System Unreliability

System definition, Failures

Aborts & Contingencies

Design, Timelines

System Vulnerability

M/OD, Redundancy

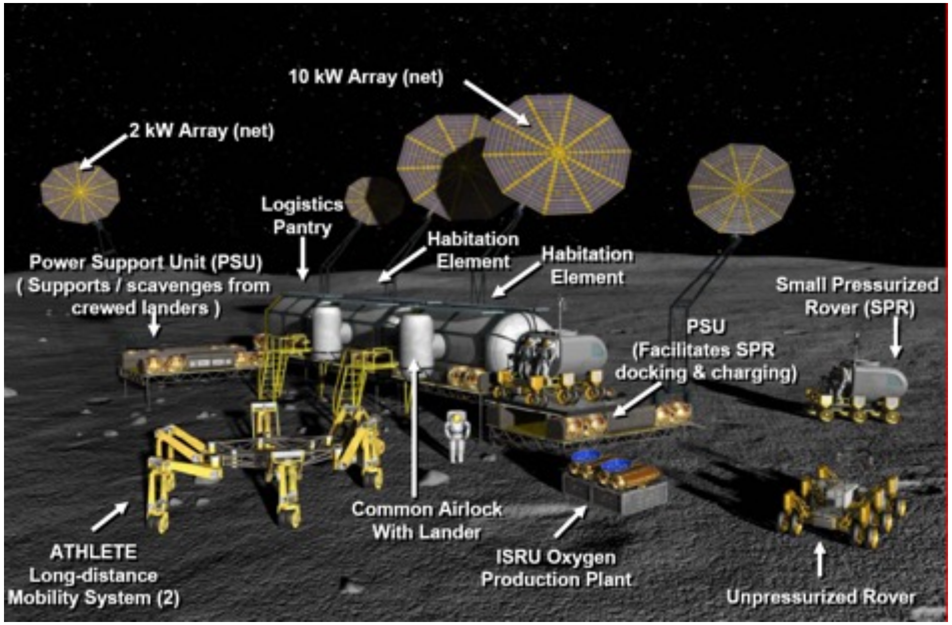
Mission risk model

OFF TO THE MOON…

LSS Background

- In 2004, NASA was chartered to return humans to the moon and enable long-term habitation
  - Baseline **transportation architecture** developed during the Exploration System Architecture Study (ESAS)
  - **Lunar surface architecture** concepts developed by Lunar Surface Systems (LSS) Project
- Campaigns: 30+ flights spanning a decade
- Combined exploration architecture driven by safety and mission success criteria

What is the probability of Loss of Mission (LOM) for a lunar campaign?

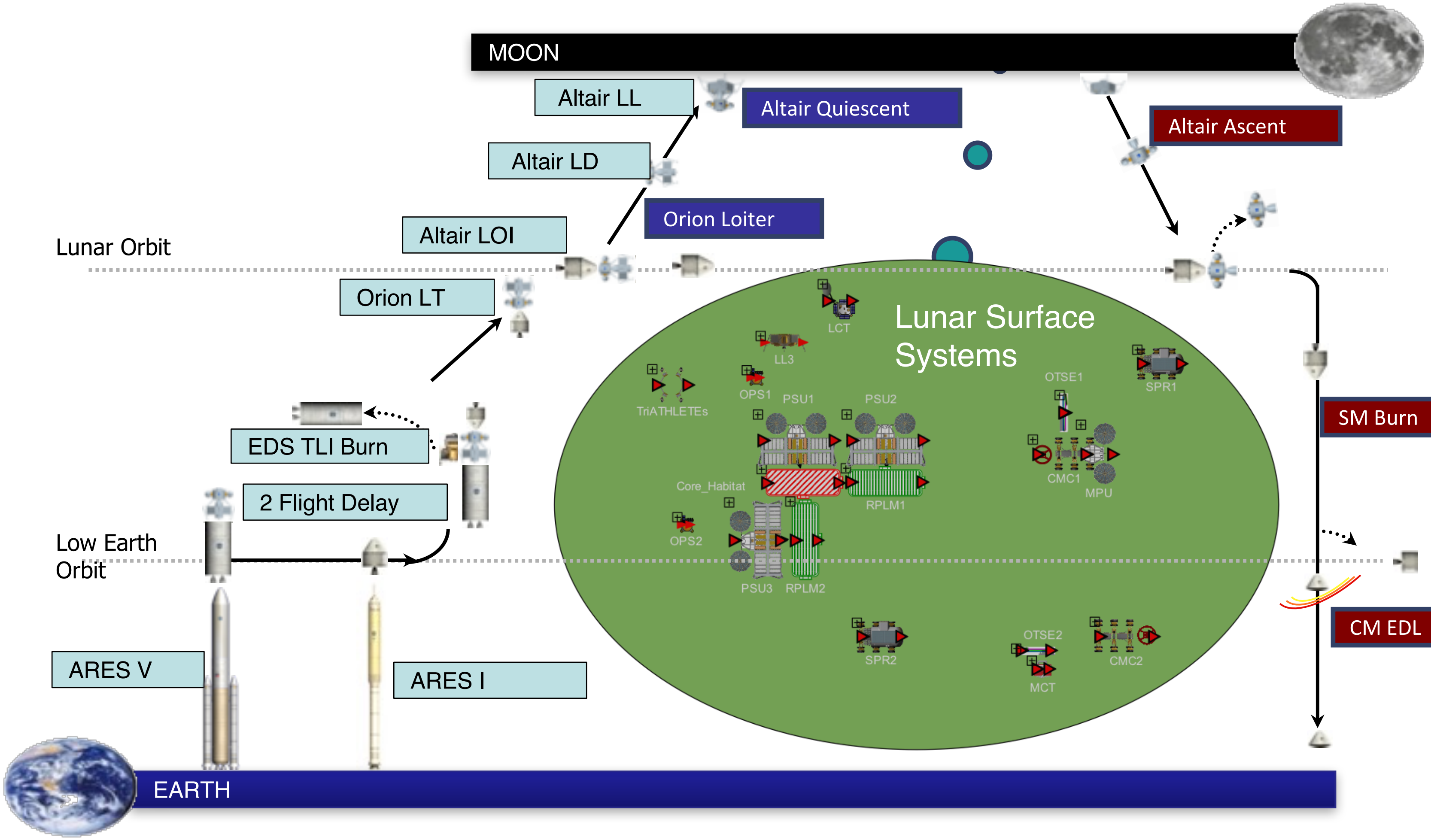


Lunar Base Loss of Mission

What is the probability of Loss of Mission over a lunar campaign?

- Proposed requirement was to be allocated as reliability requirements for Elements
- All systems required to “not fail” over duration
- Approach
  - Countered with **Availability** requirement proposal
  - Used sensitivity to scope potential ranges

Notional Lunar Mission



MOON

Altair LL

Altair Quiescent

Altair Ascent

Altair LD

Orion Loiter

Lunar Orbit

Altair LOI

Orion LT

Lunar Surface Systems

SM Burn

EDS TLI Burn

2 Flight Delay

Low Earth Orbit

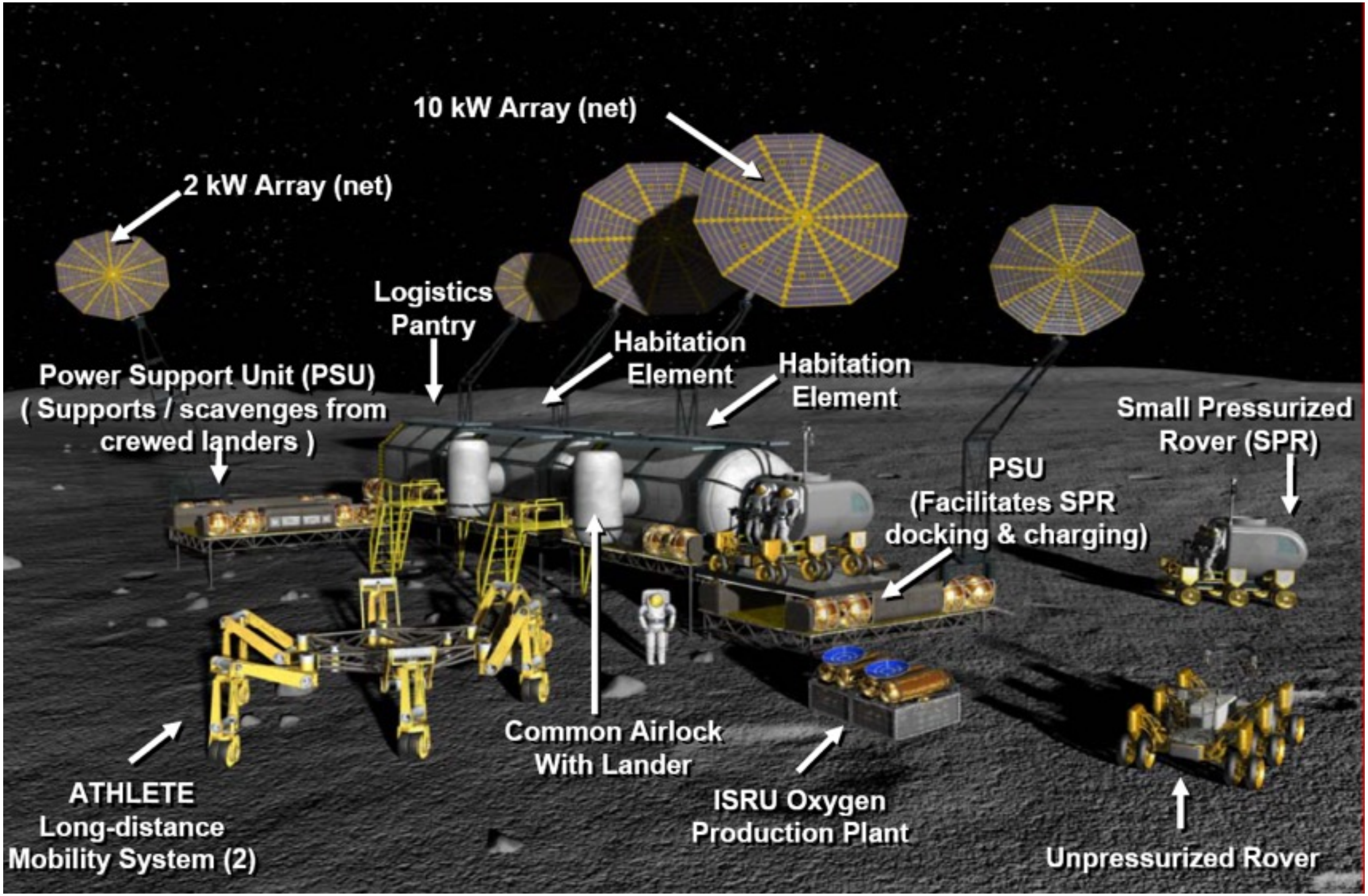
CM EDL

ARES V

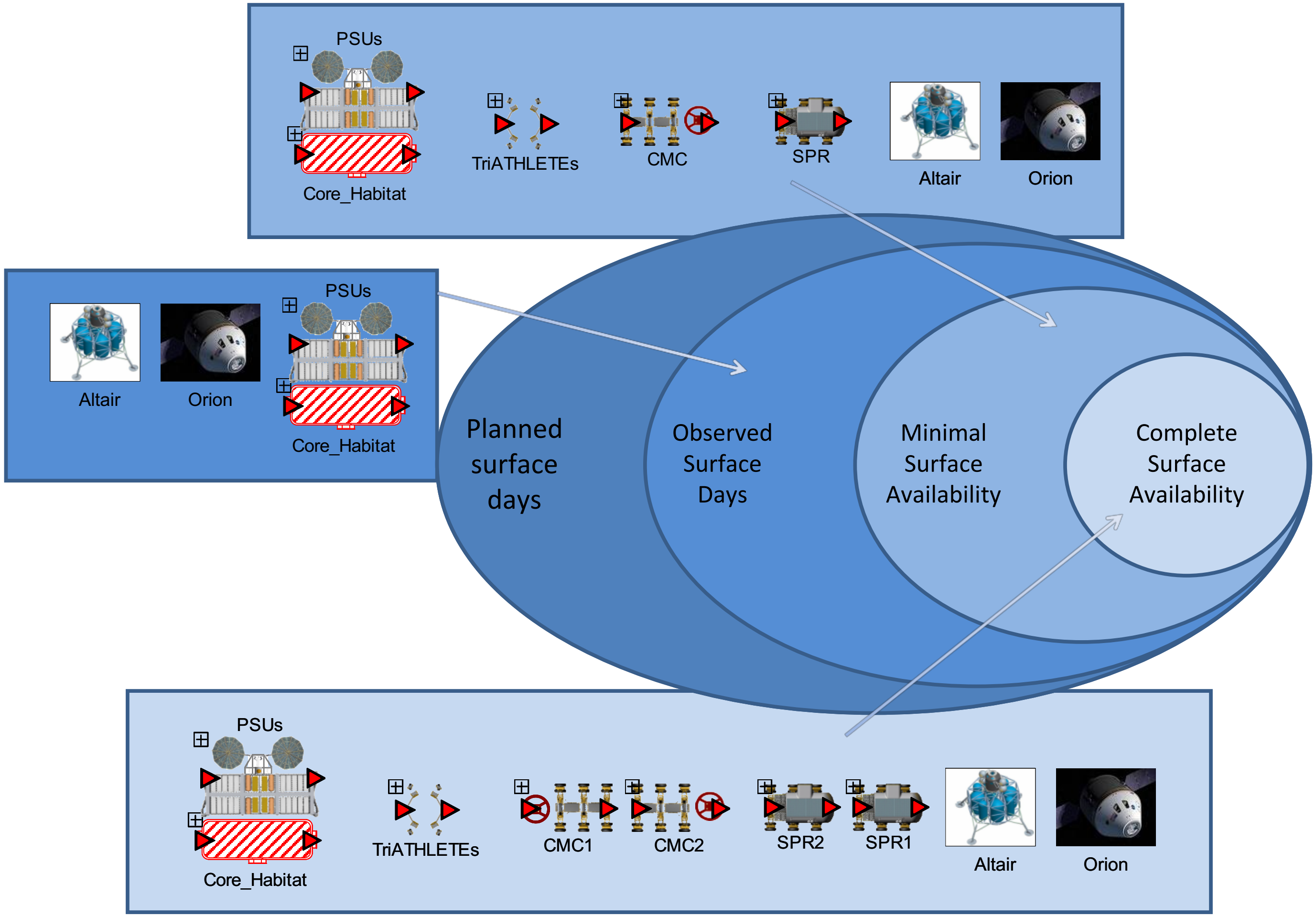
ARES I

EARTH

Lunar Surface Systems



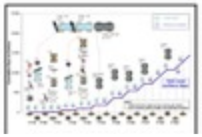
Mission Success Metrics



Integrated LSS Risk Modeling

Nominal Manifest
& Activity Timeline

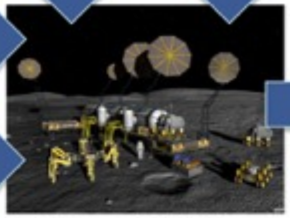
LSS Element
MELs



**Nominal delivery schedule
and mission operations**

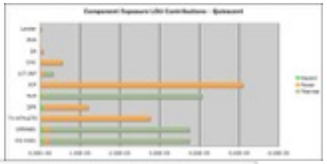
Heritage Analog
& Expert Judgment
Component Failure Data

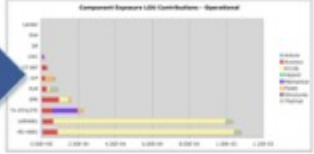
Event Reliability
Analog Classes



LSS Element Reliability Data
Rate and Demand exposures

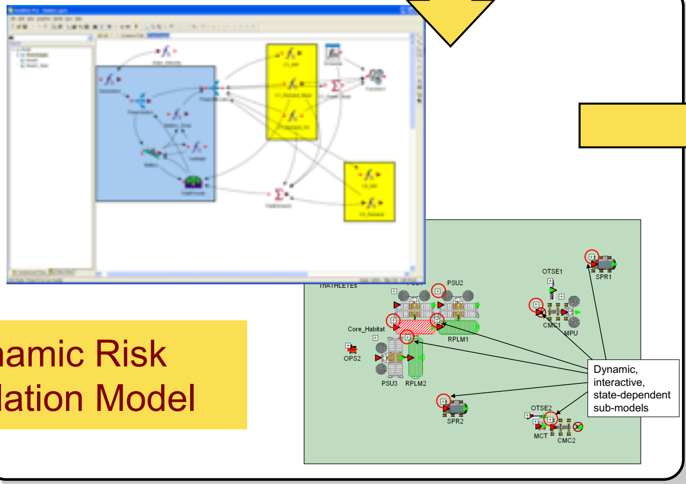
Element Reliability Data
(Initiator Likelihoods)





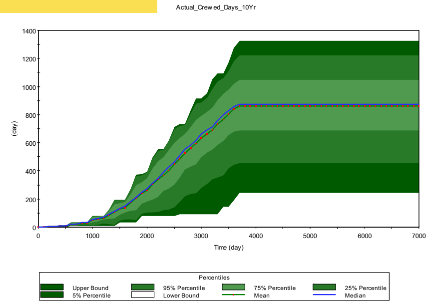
LSS Element
Reliability Data

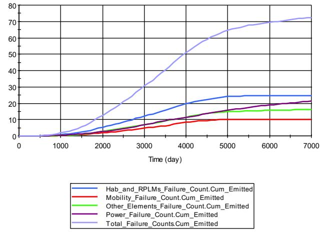
Dynamic Risk
Simulation Model

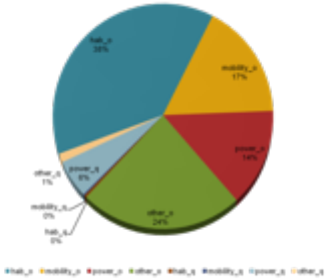


Dynamic,
interactive,
state-dependent
sub-models

Output Results



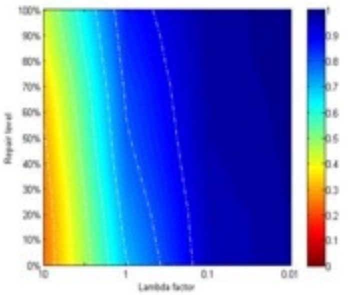




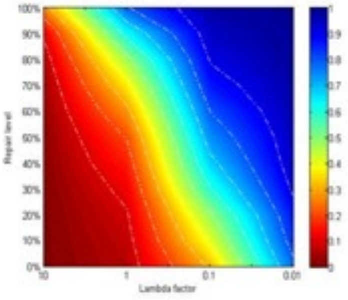
Outpost Availability Sensitivity Study

Repair assumption plays an increasingly larger role over time

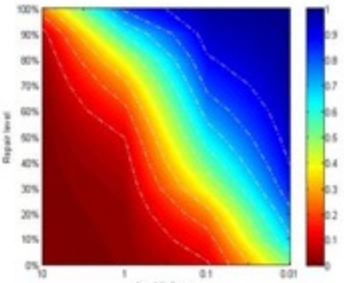
Average “complete” availability days, as a percentage of planned days



2 years operation



5 years operation



10 years operation

More repairable

More reliable

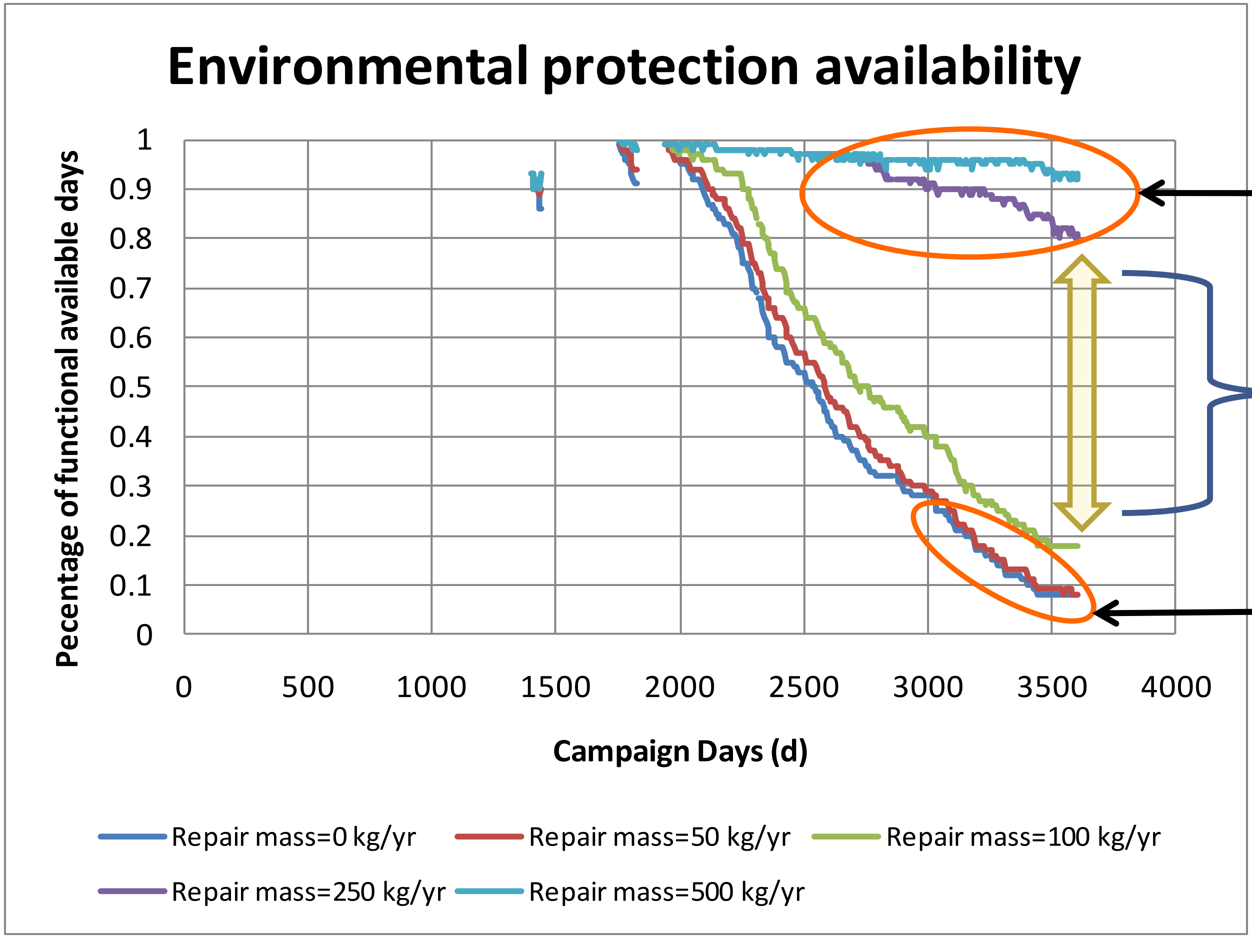
What happens with limited resupply and repairability?

- Model availability as functional capabilities within a system
  - Multiple suppliers exist from a collection of outpost elements
  - Pooled capabilities
- Failures go offline and successful repair modeled as a function of limited resources
  - Available repair mass
  - Available resources (crew presence, EVA time available)
- Sensitivity to understand levels needed

Functional Availability: Environmental Protection

Sensitivity of available days to constrained repair mass

Assumes functional environmental protection from at least one provider



Diminishing returns by increasing repair mass

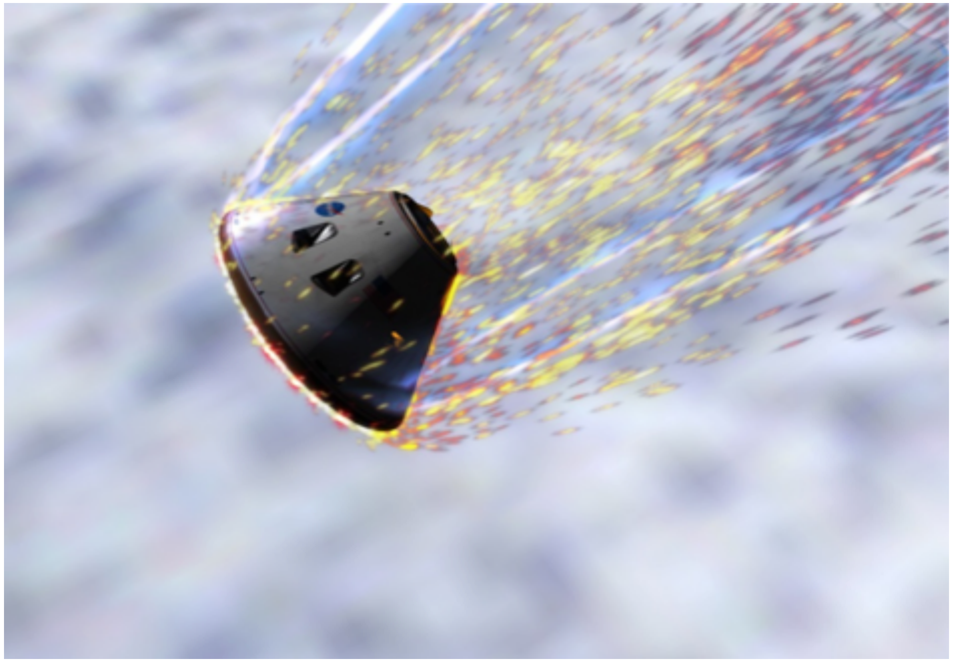
Lost availability due to insufficient repair mass

Incremental difference between no and small repair mass

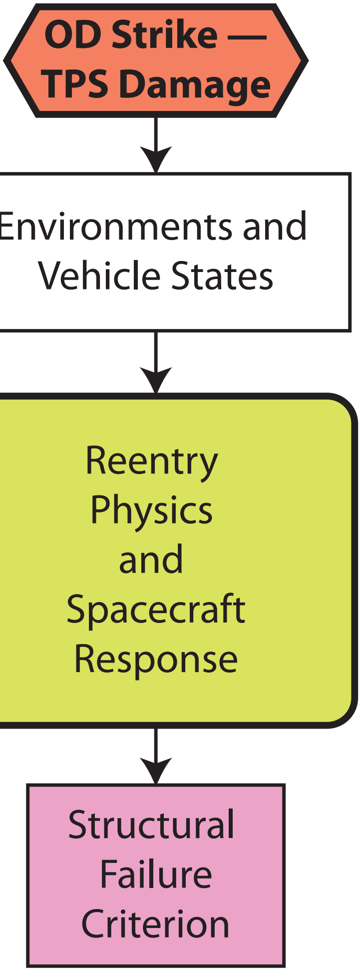
RETURN TO EARTH

Reentry Risk from Orbital Debris Strike

- What can occur?
  - Orbital debris (OD) strike damages thermal protection system (TPS) of spacecraft prior to reentry
- **What is the severity?**
  - Compromised TPS may:
    - Increase aeroheating
    - Fail to keep substructure temperature within safe limits
    - Cause structural failure and loss of crew (LOC)
- **How likely is this outcome?**
  - Depends on:
    - Likelihood of OD strike
    - Degree of TPS loss from strike
    - Degree of aeroheating increase
    - Margins in TPS and structure
    - Dispersions / uncertainties in trajectory, aeroheating, TPS



Physics-Based Risk Assessment



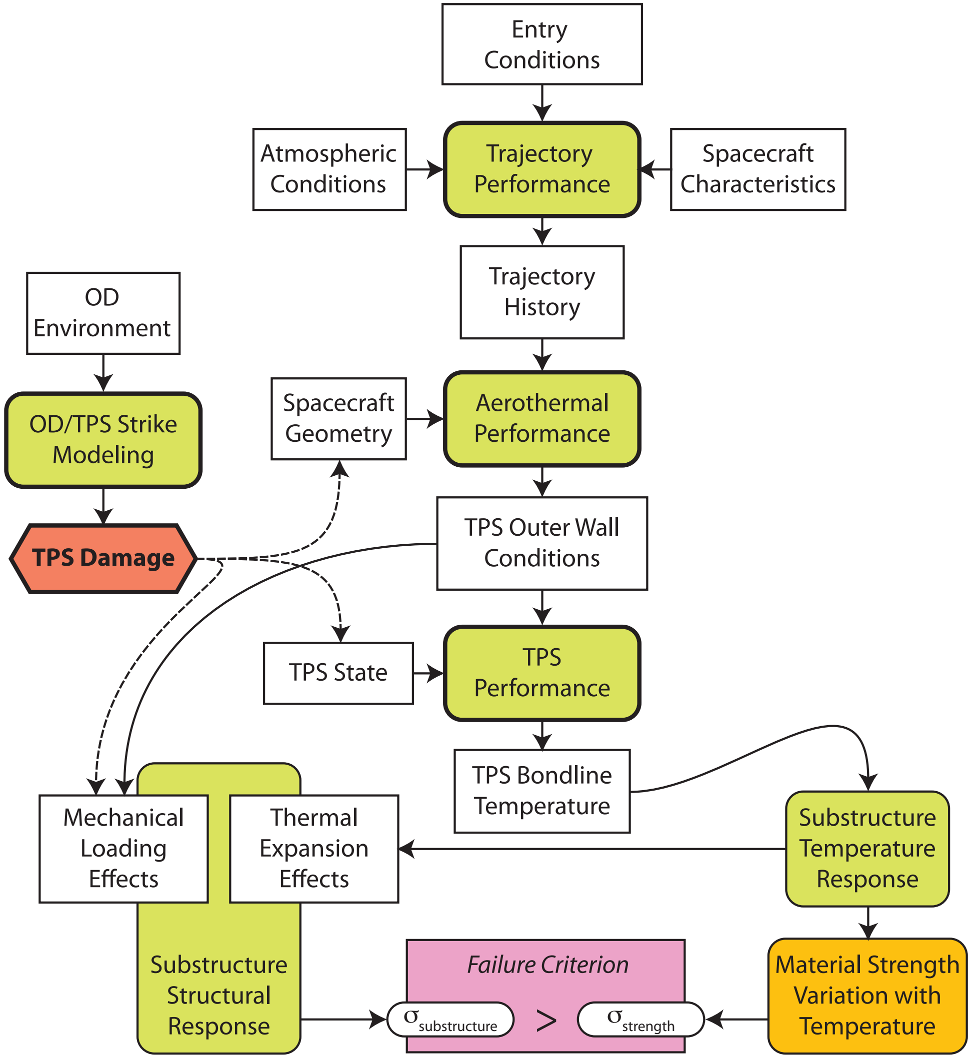
OD Strike — TPS Damage

Environments and Vehicle States

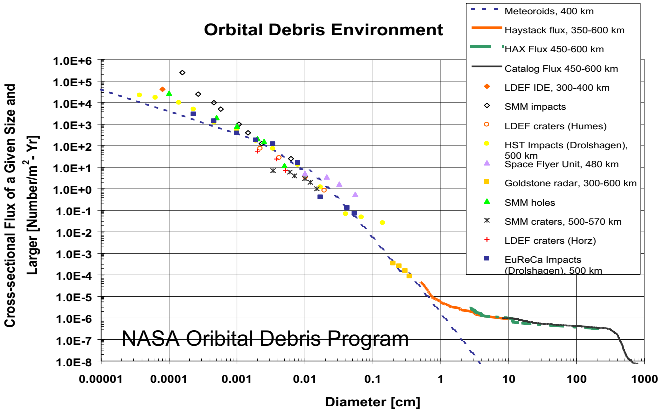
Reentry Physics and Spacecraft Response

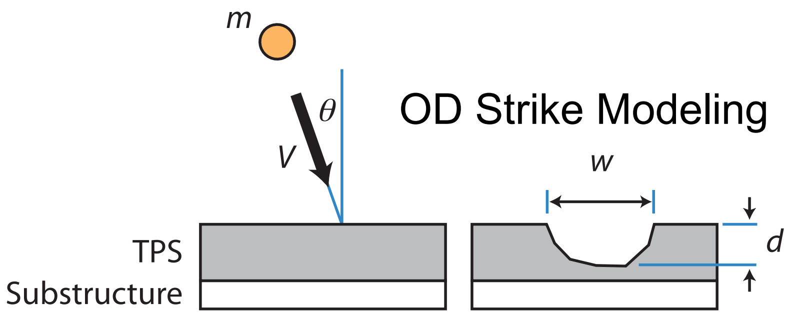
Structural Failure Criterion

Reentry Risk Framework with OD Strike

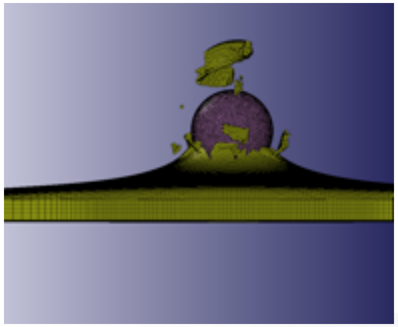


OD Strike Modeling

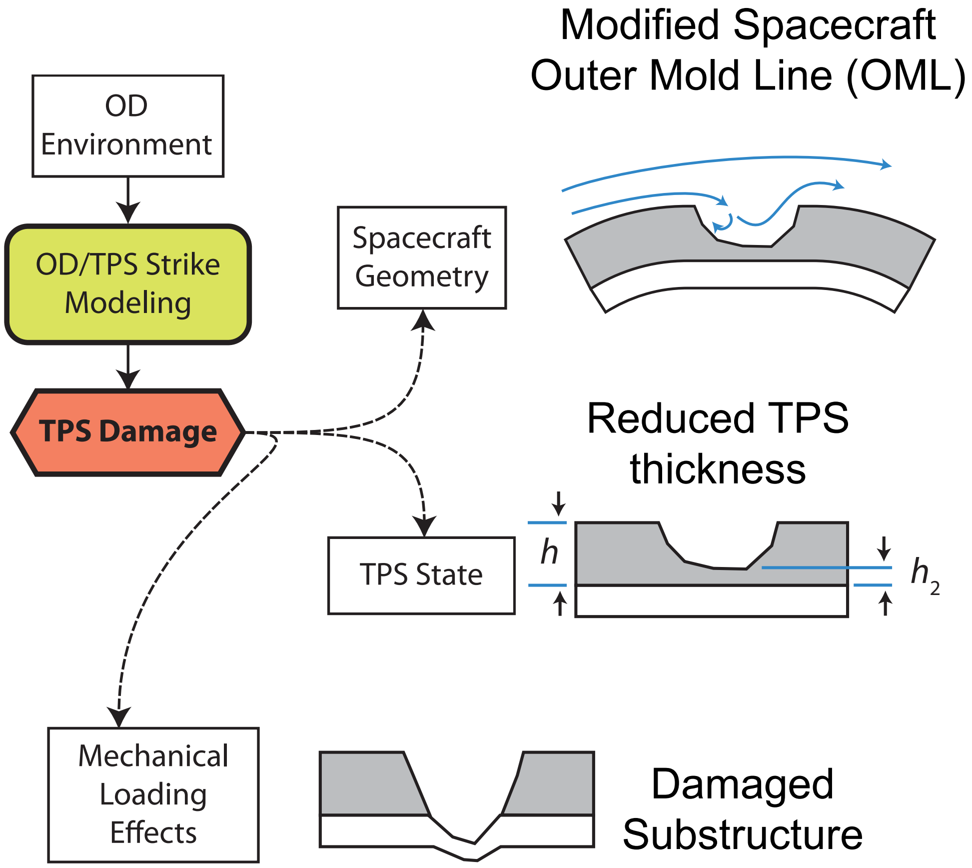




OD Strike Modeling



Impact Simulation



OD Environment

OD/TPS Strike Modeling

TPS Damage

Spacecraft Geometry

Modified Spacecraft Outer Mold Line (OML)

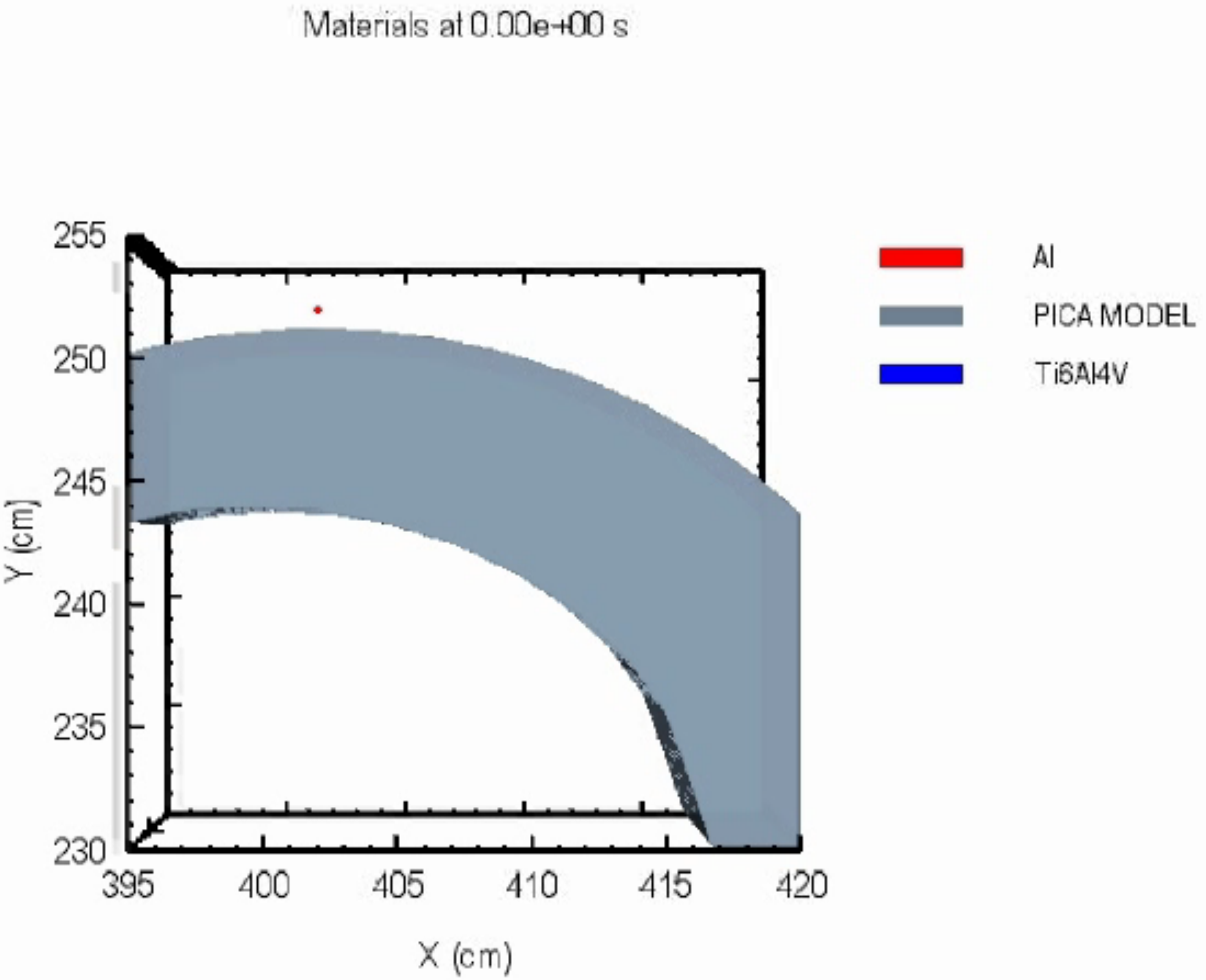
TPS State

Reduced TPS thickness

Mechanical Loading Effects

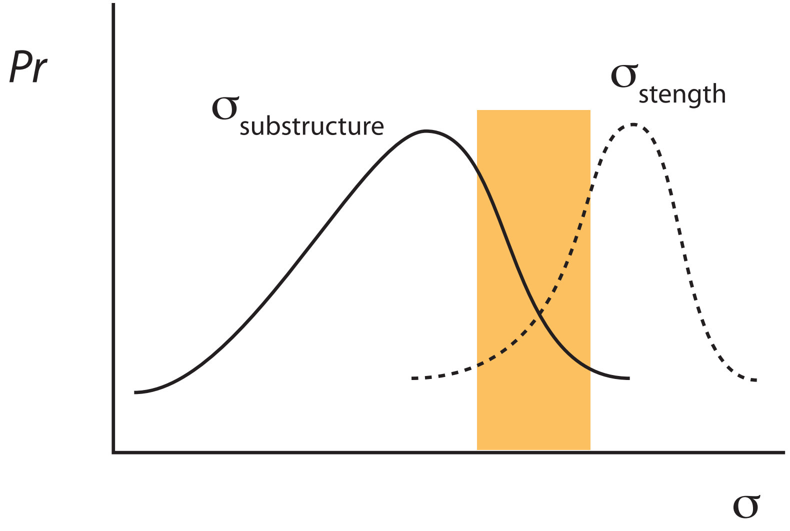
Damaged Substructure

Thermal Protection System Impact



Uncertainty in Reentry Risk Assessment

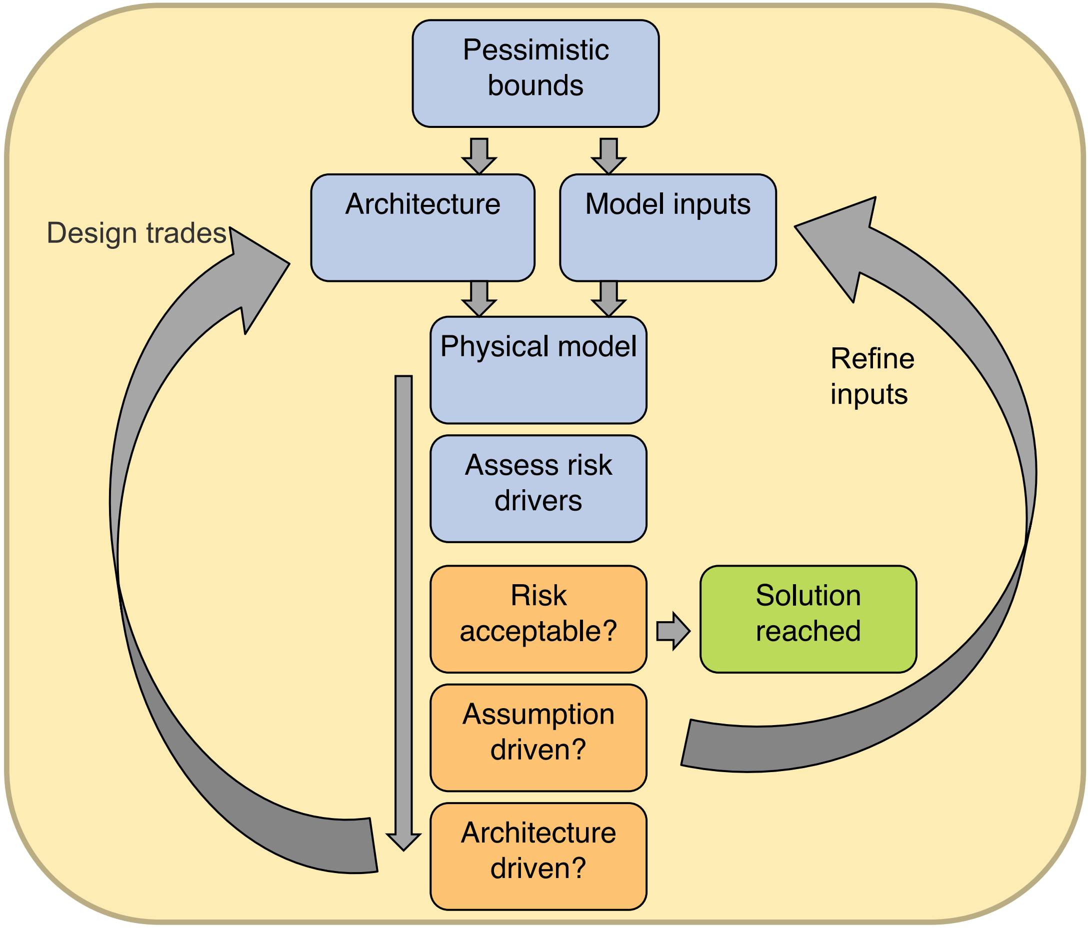
- Sources of uncertainties
  - Orbital debris: OD Environments and damage likely to be caused
  - Trajectory, aerothermal, TPS, structural analysis
    - Initial conditions
    - Atmospheric properties
    - Vehicle state and performance
    - Structural geometry and material properties
    - Models (trajectory, aerothermal, TPS) and model parameters
- Assessment must carry uncertainty through the model



Approach Application

- **Risk-informed decision support**
  - Requirement verification
  - Design optimization
  - Selection/procurement
- **Risk analysis is informative, not predictive**
  - Provides quantitative answers to specific questions
  - Always driven by specific application
  - Based on traditional methods and extended as appropriate

Iterative, responsive modeling approach



FINAL QUESTIONS?